On the Diophantine equation $y^2-k=x^3$

BY

OVE HEMER

Almqvist & Wiksells Boktryckeri AB

UPPSALA 1952

On the Diophantine equation $y^2-k=x^3$

BY

OVE HEMER

FIL. LIC., ÖSTG.

BY DUE PERMISSION OF
THE PHILOSOPHICAL FACULTY OF THE UNIVERSITY
OF UPPSALA,
TO BE PUBLICLY DISCUSSED
AT THE INSTITUTE OF MATHEMATICS,
OCTOBER 25TH, 1952, AT 10 A. M.,
FOR THE DEGREE OF DOCTOR
OF PHILOSOPHY

Almqvist & Wiksells Boktryckeri AB

UPPSALA 1952

OVE HEMER

On the Diophantine equation $y^2-k=x^3$

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41548912_0032

On the Diophantine equation $y^2-k=x^3$

BY

OVE HEMER

Almqvist & Wiksells Boktryckeri AB
UPPSALA 1952

R. UNIV.
BIBLIOTHEEK
LEIDEN

Contents

Page

Introduction 7

Chapter I. Theoretical part. Theorems and lemmata

about binary cubic forms and cubic rings 10
about the correspondence between an equation $y^2 - k f^2 = x^3$ and such forms 13
about the solubility of $(a, b, c, d) = 1$ 20
about the determination of all the solutions to $(1, p, q, r) = 1$ .. 22

Chapter II. Applications to the equations $y^2 - k f^2 = x^3$.

1. The equations $y^2 - f^2 = x^3$ 28
2. » $y^2 - 2 f^2 = x^3$ 33
3. » $y^2 - 3 f^2 = x^3$ 44
4. » $y^2 - 5 f^2 = x^3$ 51
5. » $y^2 - 6 f^2 = x^3$ 52
6. » $y^2 - 7 f^2 = x^3$ 55
7. » $y^2 - 10 f^2 = x^3$ 61
8. » $y^2 - 11 f^2 = x^3$ 63
9. » $y^2 - 13 f^2 = x^3$, $y^2 - 21 f^2 = x^3$ and $y^2 - 29 f^2 = x^3$ 65
10. » $y^2 - 14 f^2 = x^3$ 68
11. » $y^2 - 15 f^2 = x^3$ 69
12. » $y^2 - 17 f^2 = x^3$ 69
13. » $y^2 - 19 f^2 = x^3$ 72
14. » $y^2 - 31 f^2 = x^3$ 74
15. » $y^2 - 33 f^2 = x^3$ 74
16. » $y^2 - 37 f^2 = x^3$. Theorem 9 about the factorization of the prime 2 75
17. » $y^2 - 41 f^2 = x^3$ 78
18. » $y^2 - 43 f^2 = x^3$ 79
19. » $y^2 - 57 f^2 = x^3$ 79
20. » $y^2 - 65 f^2 = x^3$ 81
21. » $y^2 - 73 f^2 = x^3$ 82
22. » $y^2 - 82 f^2 = x^3$ 83
23. » $y^2 - 89 f^2 = x^3$ 84
24. » $y^2 - 97 f^2 = x^3$ 85
25. The remaining cases with $0 < k f^2 < 100$ 86
26. Some equations with $k < 0$ 88

Chapter III. The equations $y^2 + 27 k = x^3$ 90

Tables 94

Bibliography 100

In publishing this dissertation I take the opportunity to express my sincere gratitude to my distinguished teacher, Professor Trygve Nagell, who has followed my work with interest and to whom I am indebted for many good advice and stimulating criticism.

I also pronounce my particular thanks to my wife not least for putting up with me during this time.

Uppsala, August 1952.

OVE HEMER

Introduction

This equation has been the subject of many papers and has attracted great interest for more than three centuries. In 1621 Bachet stated a method of finding other rational solutions of the equation, when one was known. Fermat claimed to be the first to determine completely all the integer solutions of an equation of this type, when he declared that the equation $y^2+2=x^3$ has only one integer solution $x=3$, $y=\pm 5$, but he did not publish his method. In 1738 Euler gave an inadequate proof of this proposition, which was accepted for more than a century. He also solved the equation $y^2-1=x^3$ by applying the method of infinite descent. Important results came from V. A. Lebesgue, Jonquières, Pepin and others. A synopsis of these earlier results is given in Dickson: 'The history of the theory of numbers' II, Ch. XX, pp. 533—539.

In 1912 Mordell published an important essay [1], where he stated different methods of attacking the problem used by others and by himself. By elementary congruences he proved the insolubility of the equation in many cases. Further he applied the arithmetical theory of algebraic numbers to the equation $y^2-kf^2=x^3$, where k is square-free, in the special case that x is prime to $2kf$ and that the class number of the quadratic field $K(\sqrt{k})$ is not divisible by 3, and showed that factorization in the field $K(\sqrt{k})$ then leads to

$$y + f\sqrt{k} = \varepsilon(a + b\sqrt{k})^3, \quad x = a^2 + kb^2,$$

where a, b are rational integers and ε is a unit in $K(\sqrt{k})$. By equating irrational parts this gives certain binary cubic forms. If k is negative and $\neq -3$ these forms are reducible and the corresponding equation can easily be solved completely. Mordell, however, had no algorithm to find all solutions of irreducible forms. In his researches he also overlooked the famous theorem by Axel Thue from 1908 ([1] or [2]), that if $f(u, v)$ is an irreducible binary form of degree at least 3 with integer coefficients, then the equation

$$f(u, v) = m$$

has at most a finite number of integer solutions. The solution of the equation $y^2-k=x^3$, where the integer $k\neq 0$, can be brought back to the solution of a finite number of such equations $f(u, v)=m$, and hence $y^2-k=x^3$ has only a finite number of integer solutions. This has been proved for the more general equation

$$a y^2+b y+c=d x^n$$

where n is an integer ≥ 3, by Thue [3] with elementary methods and later by Landau and Ostrowski [1] with ideal theory. Mordell [2] has also shown that the curve

$$A x^3+B x^2+C x+D=E y^2$$

has only a finite number of integer points, if it is of genus unity, which gives the same result for our equation.

As mentioned above the problem of solving the equation $y^2-k=x^3$ is equivalent to studying certain binary cubic forms. These forms have negative or positive discriminant according as $k>0$ or <0 respectively. The next great advance is due to the very important contributions to the theory of such forms with negative discriminant which have been made by Delaunay and Nagell, independently of each others, in several papers. The most important results for us are given in the theorems 1 and 3 in this paper. They have stated methods to solve the equation $y^2-k=x^3$ and have given solutions in special cases, Delaunay for $k=2$, 3 and 5 [1] and Nagell for $k=9$ and 17 [7]. Nagell gives in his excellent monograph 'L'analyse indéterminée de degré supérieur' [5] an exposé of these results with detailed reference to the bibliography; see also the account in Th. Skolem: 'Diophantische Gleichungen' [1] Kap. VI § 3. Skolem (c.p. [1]), W. Ljunggren [1] and others have treated irreducible binary cubic forms with positive discriminant. This problem is much more difficult and there are not yet such simple and general results as in the case with negative discriminant.

In the last decades many authors have dealt with the rational (both integer and fractional) solutions of the equation. Mordell [3] has shown that the parameters of the corresponding elliptic $\wp$-function which give rational values for this function have a finite basis. Important researches have been made by Fueter [1], Nagell e.g. [5], Billing [1], Cassels [1] and others. The extensive bibliography of the whole subject in the earlier monographs by Nagell and Skolem

is completed by Cassels in the paper quoted above (published in 1950).

This paper treats mainly the case $k > 0$. I shall suggest methods of solving the equations $y^2 - kf^2 = x^3$ with k square-free and successively increasing values of f. We shall state all forms corresponding to a given equation. When f contains no odd primes which divide into two different prime ideals in the field $K(\sqrt{k})$, we shall see that we get forms all corresponding to the same cubic fields as in the case $f = 1$. I have treated these values of f for all the cases $k < 22$ and some cases more, in all 37 equations, where $kf^2 \leq 100$, which probably have not been treated before. Primes in f which divide into two different ideals give also additional forms corresponding to other fields. Table 1 gives the solutions of the equations, where $0 < kf^2 \leq 100$. Cases shown insoluble by Mordell [1] or earlier are excluded in the table. The 37 equations are solved by means of various methods and criterions mentioned at the end of chapter I. Sometimes the chosen method may not be the most conveniant but it can be an illustration of the many possibilities. There still remain 12 cases which are in fact all soluble but where the solutions are not definitely shown to be complete. They may be solved by the stated methods, once we have determined the fundamental units of the corresponding cubic fields. Table 4 gives fundamental rings and units in the treated cases of k.

Further I have treated 7 equations, where $0 < -kf^2 \leq 100$. 22 cases remain which all have solutions corresponding to irreducible forms. The results are given in table 2.

Finally I have applied results from Fueter, Billing and Cassels in the papers mentioned above, in particular table 1 by Cassels, to determine all the integer solutions of the 100 equations $y^2 + 27k = x^3$, where $0 < |k| \leq 50$, except in 11 cases. The solutions are given in table 3.

I

Theoretical part

As we pointed out in the introduction, the problem of solving the Diophantine equation $y^2 - k = x^3$ is equivalent to solving a finite number of equations

$$A U^3 + B U^2 V + C U V^2 + D V^3 = m. \tag{1}$$

By Lagrange [1] each of the equations (1) gives a certain number of equations of the form

$$a u^3 + b u^2 v + c u v^2 + d v^3 = 1. \tag{2}$$

There is still no general method of determining whether or not the number 1 can be represented by a given binary cubic form (2). We shall discuss this problem later in the section. Now let us suppose that (2) has the solution $u = u_1$, $v = v_1$. Then the substitution

$$u = u_1 x + s y, \quad v = v_1 x + t y$$

where $u_1 t - v_1 s = \pm 1$, gives an equation

$$x^3 + p x^2 y + q x y^2 + r y^3 = 1. \tag{3}$$

(2) and (3) are denoted (a, b, c, d) and $(1, p, q, r)$. They are called equivalent forms and have the same discriminant. Hence we have to find all the representations of 1 by certain given forms $(1, p, q, r)$.

If $k > 0$, (3) has a negative discriminant and we have

$$F(x, y) = x^3 + p x^2 y + q x y^2 + r y^3 = (x + \theta y)(x + \theta' y)(x + \theta'' y)$$

where θ is the real root and θ' and θ'' are the two conjugated complex roots of

$$F(x, -1) = x^3 - p x^2 + q x - r = 0. \tag{4}$$

Hence, if (4) is irreducible in the rational field, the problem is to find all the units

$$\varepsilon^n = x + \theta y \tag{5}$$

where ε is the fundamental unit of the ring $R(1, \theta, \theta^2)$ or more briefly $R(\theta)$. Results of Delaunay [1] and Nagell [3] can be comprised to

Theorem 1. *An irreducible binary cubic form with negative discriminant D and integer coefficients can give at most three representations of 1 except where $D = -44$ or -31, when there are four solutions, and where $D = -23$, when there are five solutions. A necessary condition that the form have more than two solutions is that it is equivalent to a form $(1, p, q, 1)$.*

This last condition can also be expressed

$$D(\varepsilon) \quad D(\theta)$$

where the form corresponds to the ring $R(\theta)$ with the fundamental unit ε. Then we have

Lemma 1. *If ε is the fundamental unit of $R(\theta)$ and if $D(\varepsilon) \neq D(\theta)$, then each of the corresponding equivalent forms can have at most two solutions.*

It is easily seen that all the forms $(a, b, c, d) = 1$, which correspond to a given equation $y^2 - k = x^3$, have the discriminant

$$D = -108k$$

if this number D is 6-power-free. If $108k$ is divisible by t^6, we can also get forms with the discriminant $D = -\frac{108k}{t^6}$. Delaunay has overlooked this case in [6] mom. 23. Hence D is always even if $k \not\equiv 2^{6n-2} \pmod{2^{6n-1}}$, $n = 1, 2, \ldots$

If $F = (1, p, q, r) = 1$ we have

$$D(F) = D = p^2q^2 + 18pqr - 4q^3 - 4rp^3 - 27r^2. \tag{6}$$

Now suppose that D is even and $D(\varepsilon) = D(\theta) = D$. Then, by (6), (3) is equivalent to

$$X^3 + PX^2Y + QXY^2 + Y^3 = 1 \tag{7}$$

where both P and Q are odd. Starting from (7) we get (3) by a unimodular substitution

$$X = ax + by, \quad Y = cx + dy. \tag{8}$$

This implies that

$$a^3 + P a^2 c + Q a c^2 + c^3 = 1$$

i.e. (a, c) must be a solution of (7). Here $a \equiv c \pmod 2$ and since $ad - bc = \pm 1$ we get either

$$a \text{ even, } c \text{ and } b \text{ odd, } p \equiv q \equiv r \equiv d \pmod 2$$

or

$$c \text{ even, } a \text{ and } d \text{ odd, } p \equiv q \equiv r \equiv b \pmod 2.$$

Then we have

Lemma 2. *A binary cubic form $(1, p, q, r)$ with even discriminant and with $p \equiv q \pmod 2$ corresponds to a ring $R(\theta)$, where $D(\varepsilon) \neq D(\theta)$, and hence has at most two solutions, if $D < 0$.*

Further if we put $(a, c) = (1, 0)$ or $(0, 1)$, (8) gives forms (3), where $\varepsilon = x \pm \theta$ in the corresponding ring, which can easily be verified. If (7) has a third solution (a, c), (8) gives a form with the solutions $(1, 0)$, $(\mp b, \pm a)$ and $(\pm d, \mp c)$ where $ad - bc = \pm 1$. Then if $|a|$ and $|c| \neq 1$, the fundamental unit of $R(\theta)$, defined by (4), cannot be of the type $x \pm \theta$. Hence

Lemma 3. *A cubic ring $R(\theta)$, where $D(\varepsilon) = D(\theta)$ but ε is not of the type $x \pm \theta$, corresponds to a form $(1, p, q, r)$ with exactly three solutions, if D is negative and $\neq -23$, -31 or -44. If this form has the solutions $(1, 0)$ and (x_1, y_1) then the third solution (x_2, y_2) satisfies*

$$x_1 y_2 - y_1 x_2 = \pm 1. \tag{9}$$

The last part of the lemma is an immediate inferrence from the fact that the solution (a, c) of (7) corresponds to the solution $(1, 0)$ of (3) and that $|x_1 y_2 - y_1 x_2|$ is an invariant by the substitution. Hence this relation (9) is generally not true, if ε is of the type $x \pm \theta$. (9) gives another proof of lemma 2, since $p \neq q \pmod 2$ implies that $y \equiv 0 \pmod 2$ in (3) and hence (9) can never be satisfied.

Sometimes (9) may be used to decide that a form (3), where $p \equiv q \pmod 2$, can have at most two solutions. For instance the solution of the equation $y^2 - 33 = x^3$ leads to the only soluble form $(1, 0, 6, 10) = 1$. Suppose that this form has the three solutions $(1, 0)$, (u_1, v_1) and (u_2, v_2). There is no solution with $|v| = 1$. We have either $v \equiv 0 \pmod 5$ and $u \equiv 1 \pmod 5$ or $v \equiv \pm 2 \pmod 5$ and $u \equiv 2 \pmod 5$. Hence $u_1 v_2 - u_2 v_1 \not\equiv \pm 1 \pmod 5$ and the form and so the equation

$y^2-33=x^3$ can have at most two solutions. In fact there is only one solution, as we shall prove later in this paper.

By the examination of the equations $y^2-kf^2=x^3$, where k is square-free, we distinguish the cases $k=1$ and $k\neq 1$. If $k=1$ we have

Theorem 2. *If $2f$ contains r different primes, then the solution of the equation $y^2-f^2=x^3$ can be replaced by the solution of the reducible form $u^3+v^3=2f$ and $\frac{3^r-1}{2}$ irreducible forms of the type Au^3+Bv^3, all corresponding to different cubic fields $K\left(\sqrt[3]{\frac{A}{B}}\right)$.*

Proof. We can write

$$\pm y+f=au^3$$
$$\pm y-f=bv^3$$

where ab is the cube of a divisor of $\prod_{i=1}^{r} p_i$. Then we get the forms by subtraction and it is easy to see that the number of irreducible forms is $\sum_{j=1}^{r} 2^{j-1}\binom{r}{j}=\frac{3^r-1}{2}$ and that they all belong to different fields. For instance the equation $y^2-225=x^3$ has $2f=2\cdot 3\cdot 5$ and can be replaced by the forms

$u^3+v^3=30$, $u^3-2v^3=15$, $u^3+3v^3=10$, $u^3+5v^3=6$, $u^3+6v^3=5$,
$2u^3+3v^3=5$, $u^3+10v^3=3$, $2u^3+5v^3=3$, $u^3+15v^3=2$, $3u^3+5v^3=2$,
$u^3+30v^3=1$, $2u^3+15v^3=1$, $3u^3+10v^3=1$ and $6u^3+5v^3=1$.

This gives immediately 9 solutions of the equation. We have great use of the following theorem by Nagell [1, 2]:

Theorem 3. *The Diophantine equation*

$$Au^3+Bv^3=C$$

where A, B and C are rational integers and $C=1$ or 3, with a single exception has at most one solution in integers u and v different from 0. The only exception is the equation $2u^3+v^3=3$, which has the two solutions $(1, 1)$ and $(4, -5)$. These non-trivially soluble forms correspond all to different fields with the exception that $K(\sqrt[3]{2})$ and $K(\sqrt[3]{20})$ contain 3 and 2 of them respectively.

It is always possible to determine the eventually solution of a form $Au^3+Bv^3=C$ with $C=1$ or 3, because it can be replaced by a finite number of forms $u^3+dv^3=1$. Delaunay [5] has shown that such forms have at most one non-trivial solution and that if there is a solution $u=u_1$, $v=v_1$, then $u_1+v_1\sqrt[3]{d}$ is the fundamental unit of the ring $R(\sqrt[3]{d})$ (and except in some cases, of the field $K(\sqrt[3]{d})$, as Nagell [1] has shown). Forms where $C\neq 1$ or 3 may sometimes be solved by specially methods. For instance we can always write the form $U^3+dV^3=m$, which implies that $U+V\cdot\sqrt[3]{d}=\varepsilon^n\cdot\alpha$, where ε is the fundamental unit of $R(\sqrt[3]{d})$ and α is an integer of the ring with the norm m. Then the coefficient of $\sqrt[3]{d^2}$ must vanish in the right member. Otherwise we can replace $Au^3+Bv^3=C$ by a finite number of forms $(a, b, c, d)=1$ and treat them by methods mentioned in the following.

If $k\neq 1$ we suppose without losing the general applicability that (f, x^3) is cube-free. Then we have the theorems:

Theorem 4. *If $2f$ contains no prime which divides into two different prime ideals in the field $K(\sqrt{k})$, then all the integer solutions of the equation*

$$y^2-kf^2=x^3$$

are contained in the $\dfrac{3^{e+1}\mp 1}{2}$ *different equations*

$$N(\beta_i)\cdot(\pm y+f\sqrt{k})=\eta\cdot\beta_i\cdot\alpha^3$$

where (β_i), $i=1, 2, \ldots, 3^e$, is the cube of arbitrary ideals, one from each of the 3^e classes C_i with the property $C_i^3=(1)$, α is an integer in $K(\sqrt{k})$ and $\eta=1$ or ε, where ε is the fundamental unit of $K(\sqrt{k})$ (or an arbitrary unit which is not a cube). *e is the basis number for 3 in the group of ideal classes.*

Proof. We get immediately

$$\pm y+f\sqrt{k}=\mathfrak{a}^3.$$

Since $\mathfrak{a}^3$ is a principle ideal, we can always choose $\mathfrak{b}_i$, $i=1, 2, \ldots, 3^e$, as an arbitrary ideal from one of the 3^e ideal classes C_i with the

property $C_i^3 = (1)$ such that $\mathfrak{b}_i \mathfrak{a} = (\alpha)$ is a principle ideal. Then multiplication with $N(\beta_i)$, where $\beta_i = \mathfrak{b}_i'^3$, gives the result of the theorem. Since there are the principal ideal class and $\frac{3^e - 1}{2}$ pairs of conjugated classes, we get $\frac{3^e + 1}{2}$ equations if $k < 0 \neq -1$ or -3 and $2 + 3 \cdot \frac{3^e - 1}{2} = \frac{3^{e+1} + 1}{2}$ equations if $k > 1$.

If the class number $h(K(\sqrt{k}))$ is not divisible by 3, we have $e = 0$ and get

$$\pm y + f\sqrt{k} = \eta \alpha^3$$

where $\eta = 1$ or ε, if $k > 1$, and $\eta = 1$, if $k < 0$ and also $\eta = \sqrt{-1}$ and $\frac{1 + \sqrt{-3}}{2}$ if $k = -1$ or -3. Hence we only get reducible forms if $k < 0 \neq -3$. Specially we observe that if $k \equiv 5 \pmod 8$ and $f \not\equiv 4 \pmod 8$ and if ε has the form $\frac{a + b\sqrt{k}}{2}$, a and b odd integers, then only the easily examined case $\eta = 1$ can give solutions. This follows, since α^3 must have the form $a + b\sqrt{k}$, and because x is odd, $\varepsilon \alpha^3$ cannot have this form. Then 37, 80 and — 48 are the only values of kf^2 numerical less than 100, where we can get soluble irreducible forms.

If the group of ideal classes is cyclic (and I know no case, where it is not, when $k > 0$), we have $e = 1$, if $h(K(\sqrt{k}))$ is divisible by 3, and we can find a prime $p = \mathfrak{p} \cdot \mathfrak{p}'$, where $\mathfrak{p}$ is not a principal ideal and $\mathfrak{p}^3 = (\beta)$. This gives if $k > 1$ the five equations

$$\pm y + f\sqrt{k} = \eta \alpha^3$$

$$p^3 (\pm y - f\sqrt{k}) = \eta \beta \alpha^3$$

$$p^3 (\pm y + f\sqrt{k}) = \varepsilon \beta' \alpha^3$$

where $\eta = 1$ or ε, and if $k < 0$ the two equations

$$\pm y + f\sqrt{k} = \alpha^3$$

$$p^3 (\pm y + f\sqrt{k}) = \beta \alpha^3.$$

Theorem 5. *If $2f$ contains r different primes p_i, $i = 1, 2, \ldots, r$, which divide into two different prime ideals in the field $K(\sqrt{k})$, and*

if the class number $h(K(\sqrt{k}))$ is not divisible by 3, then all the integer solutions of the equation

$$y^2 - k f^2 = x^3$$

are contained in the equations

$$\prod_{i=1}^{r} p_i^{q_i} (\pm y + f\sqrt{k}) = \prod_{i=1}^{r} \mathfrak{p}_i^{h_i} \alpha^3 \cdot \eta \beta \alpha^3$$

where $h_i = 0$ or the least positive integer making $\mathfrak{p}_i^{h_i}$ a principle ideal and all the combinations of these values are considered. If $h_i = 0$ we put $q_i = 0$, and if $h_i > 0$ and hence $\equiv 0 \pmod 3$, we put $q_i = h_i - 2$, if $h_i \equiv 1 \pmod 3$, and $q_i = h_i - 1$, if $h_i \equiv -1 \pmod 3$. α is an integer in $K(\sqrt{k})$ and $\eta = 1$, ε or ε'. The number of different equations is $\frac{1}{2}(3^{r+1}+1)$, if $k > 1$ or $= -3$, and $\frac{1}{2}(3^r+1)$, if $k < 0$ $\neq -1$ or -3. $k = -1$ gives $3^r + 1$ equations.

Proof. Suppose $p_i | x$ and let $p_i^{m_i}$ be the highest power of p_i that divides f ($0 \leq m_i \leq 2$, since (f, x^3) is cube-free). Then we easily see that x must be divisible by $p_i^{m_i}$. Put $x = n x_1$, $y = n y_1$ and $f = n f_1$, where $n = \prod_{p_i | x} p_i^{m_i}$. We get

$$y_1^2 - k f_1^2 = n x_1^3 .$$

$p_i \nmid f_1$ and we have generally

$$\pm y_1 + f_1 \sqrt{k} = \Pi \mathfrak{p}_i^{m_i} \mathfrak{a}^3 .$$

If $k \equiv 1 \pmod 8$ and $2 = p_1$, we can also get, if $2^2 | f$

$$\pm y_1 + f_1 \sqrt{k} = 2 \cdot \prod_{i=1} \mathfrak{p}_i^{m_i} \mathfrak{a}^3$$

and if f is odd

$$\pm y_1 + f_1 \sqrt{k} = 2 \mathfrak{p}_1 \Pi \mathfrak{p}_i^{m_i} \mathfrak{a}^3 .$$

By multiplication with n all the three cases give equations of the type

$$\pm y + f\sqrt{k} = \Pi \mathfrak{p}_i^2 \mathfrak{p}_i' \mathfrak{a}^3 .$$

Finally multiplication with $\prod_{p_i | x} p_i^{q_i}$ gives the result of the theorem. To determine the number of equations we observe that $\mathfrak{p}_i \neq \mathfrak{p}_i'$. Hence β can get $1 + \sum_{j=1}^{r} 2^{j-1} \binom{r}{j} = \frac{1}{2} \cdot (3^r + 1)$ different non-conjugated values and we have just so many equations if $k < 0 \neq -1$ or -3 and $2 + 3 \cdot \sum_{j=1}^{r} 2^{j-1} \binom{r}{j} = \frac{1}{2} \cdot (3^{r+1} + 1)$ equations if $k > 1$.

It does not present much difficulty to extend theorem 5 to cases, where $h(K(\sqrt{k}))$ is divisible by 3, but the general expression is more complicated and we have no use for it in this paper. The corresponding equations can be determined in a similar way as in the proof by Landau and Ostrowski [1] that the equation $y^2 - k = x^3$ has a finite number of integer solutions. The result of theorem 4 is of course included in theorem 5, if we put $r = 0$. It is also clear that all forms which may be derived from one of the equations in theorem 4 or 5 by linear substitutions with integer coefficients of a and b in α, correspond to rings belonging to the same cubic field.

Further we shall nearer consider the often occurring equation

$$\pm y + f\sqrt{k} = \varepsilon(a + b\sqrt{k})^3$$

where f is square-free and $\varepsilon = A + B\sqrt{k}$, A and B integers. This gives

$$F(a, b) = Ba^3 + 3Aa^2b + 3Bkab^2 + Akb^3 = f. \tag{10}$$

We shall prove the following theorem:

Theorem 6. *If f is square-free and contains s primes > 3 and if $A + B\sqrt{k}$ is a unit, then, if F is soluble, the number of forms*

$$G(u, v) = 1$$

which substitute (10), are at most 3^s, if f is odd, and $2 \cdot 3^s$, if f is even. The rings which correspond to the forms $G = 1$ belong all to the same cubic field as the ring corresponding to the form $F = 1$.

Proof. Let (a_1, b_1) be a solution of (10). Then the substitution

$$a = a_1 u + cv, \quad b = b_1 u + dv$$

where $a_1 d - b_1 c = \pm 1$, gives

$$F_1(u, v) = (f, p, q, r) = f.$$

If then $3 \mid f$, we get the condition $rv^3 \equiv 0 \pmod 3$, since p and q are divisible by 3. Either $r \equiv 0$ or $v \equiv 0 \pmod 3$ this gives only one form $\left(\frac{f}{3}; p_1, q_1, r_1\right) = \frac{f}{3}$. Hence we can suppose $(3, f) = 1$ and further we suppose that f, p, q and r have no common divisor, because this can give the largest number of forms G. Now suppose at first $(v, f) = 1$ and let u_1 be a solution of the congruence

(11) $$F_1(u, 1) \equiv 0 \pmod{f}.$$

Then the substitution $u = u_1 v - f w$ gives

$$F_1(u, v) = F_1(u_1 v - f w, v) = f \cdot G(v, w) = f.$$

Conversely it is easily seen that this relation implies $F_1(u_1, 1) \equiv 0 \pmod{f}$. Let u_2 be another solution of (11)

$$u_2 \not\equiv u_1 \pmod{f}.$$

Then

$$(u_2 - u_1)[p(u_2 + u_1) + q] \equiv 0 \pmod{f}$$

and if

$$(u_2 - u_1, f) = d, \quad f = d f'$$

we get

$$p(u_2 + u_1) + q \equiv 0 \pmod{f'}$$

$(p, f') = d_1 > 1$ implies that $(r, d_1) = 1$ and hence that (11) is insoluble. Then

$$(p, f') = 1$$

and if $p p' \equiv 1 \pmod{f'}$ we get

$$u_2 \equiv -u_1 - p' q \pmod{f'}.$$

Now let u_3 be another solution of (11), which satisfies $(u_3 - u_1, f) = d$, and put

$$u_2 = u_1 + k_2 d, \quad u_3 = u_1 + k_3 d.$$

This gives

$$d(k_3 - k_2) \equiv 0 \pmod{f'}$$

and since f is square-free

$$k_3 - k_2 \equiv 0 \pmod{f'} \text{ and } u_3 - u_2 = d(k_3 - k_2) \equiv 0 \pmod{f}.$$

Hence, if u_1 is a given solution of (11), we can have at most one solution $u_2 \not\equiv u_1 \pmod{f}$ such that $(u_2 - u_1, f) = d$. Then, if f is odd and contains s primes > 3, we get at most

$$\sum_{i=0}^{s} \binom{s}{i} = 2^s$$

solutions of (11), if $(v, f) = 1$. Since $(v, f) = p_1 \cdot p_2 \cdot \cdots \cdot p_j$ gives a form with at most 2^{s-j} solutions to the corresponding congruence (11), we get the maximal number m of the forms G

$$m = \sum_{j=0}^{s} \binom{s}{j} \cdot 2^{s-j} = 3^s.$$

Further it can be shown that $f=2f_1$ in (10) only can give two forms $F'=f_1$ and then the theorem is proved, because the last part is trivial. Specially we see that $f=1$ and 3 give only one form.

By lemma 2 and the theorems 4 and 6 we can now prove

Theorem 7. *If $k>0$ is square-free and $\equiv 1 \pmod 4$, if f is square-free and odd and not containing primes, which divide into different prime ideals in $K(\sqrt{k})$ and if the class-number $h(K(\sqrt{k}))$ is not divisible by 3, then the equation*

$$y^2-kf^2=x^3$$

except the very few and easily determined solutions, corresponding to the reducible form $3a^2b+kb^3=f$, can have at most $2\cdot 3^s$ solutions, where s is the number of primes >3, which divide f. Specially, if $f=1$ or 3, there can be at most two solutions.

Proof. By theorem 4 we have to examine only one form (10). Let (a_1, b_1) be a solution of this form. Then the substitution

$$a=a_1u+cv, \quad b=b_1u+dv$$

where

$$a_1d-b_1c=\pm f$$

gives a form

$$u^3+\frac{3p}{f}\cdot u^2v+\frac{3q}{f}\cdot uv^2+\frac{r}{f}\cdot v^3=1$$

which has integer coefficients and is equivalent to one of the forms $G(u, v)=1$ discussed in theorem 6. Then by lemma 2 it is sufficient to show that

$$p\equiv q \pmod 2.$$

We have

$$p=Ba_1^2c+Aa_1^2d+2Aa_1b_1c+2kBa_1b_1d+kBb_1^2c+kAb_1^2d$$

and

$$q=Ba_1c^2+Ab_1c^2+2Aa_1cd+2kBb_1cd+kBa_1d^2+kAb_1d^2$$

i.e. we shall show that

$$A(a_1^2d-b_1c^2)\equiv kB(a_1d^2-b_1^2c) \pmod 2$$

or, since $f=\pm(a_1d-b_1c)$ is odd

$$A\equiv kB \pmod 2$$

which is satisfied, since $A+B\sqrt{k}$ is a unit.

For instance $k=15$ satisfies the conditions of theorem 7 and hence the equation $y^2-15=x^3$ is completely solved by the two known solutions $(1, \pm 4)$ and $(109, \pm 1138)$.

Returning to the task of finding all the integer solutions of a given binary cubic form with negative discriminant we shall at first discuss the not yet generally soluble problem of deciding, whether a form $(a, b, c, d)=1$ is equivalent to a form $(1, p, q, r)=1$ or not, i.e. whether it has solutions or not. It is often possible to show the impossibility of $(a, b, c, d)=1$ by congruences, generally modulo 7 or 9, where ± 1 are the only cubic rests (cp Mordell [1]). If this fails we can go on in the following way:

$F(u, v)=(1, p, q, r)=1$ implies that $(1, p, q, r)=N(u+v\theta)$ where $u+v\theta$ is a positive unit and θ is defined by

$$\theta^3-p\theta^2+q\theta-r=0. \tag{4}$$

As Delaunay has pointed out (cp [4] t. 1, p. 258) the unimodular transformation

$$(1, p, q, r)\cdot\begin{pmatrix} A & B \\ C & D \end{pmatrix}\rightarrow(a, b, c, d) \tag{12}$$

where

$$AD-BC=1$$

implies that

$$(a, b, c, d)=N(\lambda U+\mu V)$$

where

$$\lambda=A+C\theta, \quad \mu=B+D\theta$$

and $\lambda U+\mu V$ is a positive unit of $R(\theta)=R(1, \alpha, \beta)$, if we as usual define

$$\begin{aligned} &\alpha^3-b\alpha^2+ac\alpha-a^2d=0 \\ &\beta^3-c\beta^2+db\beta-d^2a=0 \\ &\alpha\beta=ad. \end{aligned} \tag{13}$$

That the modul $M(1, \alpha, \beta)$ is a ring and that (a, b, c, d) corresponds to this ring $R(1, \alpha, \beta)$ is proved by Levi [1] and Delaunay [3] and also by Nagell [6] Satz XI and XII. Then

$$\frac{\mu}{\lambda}=\frac{\alpha}{a}$$

and $a=\lambda j$, $\alpha=\mu j$. Now $Da-C\alpha=(D\lambda-C\mu)\cdot j=j$ and hence j is an algebraic integer in $R(1, \alpha, \beta)$ and we get

$$\lambda = \eta \cdot \frac{a}{j}, \qquad \mu = \eta \cdot \frac{\alpha}{j}$$

where η is a unit in $R(1, \alpha, \beta)$. A necessary (but not sufficient) condition for the relation (12) is that such integers λ and μ exist, i.e. that (j) and hence (λ) and (μ) are principle ideals of $R(1, \alpha, \beta)$. Since $(\lambda, \mu) = 1$ (we can suppose that the form is primitive), we have

$$(\alpha, a) = (j)$$

and it is always possible to examine, whether this is a principle ideal in the ring or not and to determine it. Very often we can use the following lemma:

Lemma 4. *If $(a, d) = 1$ we get $N\lambda = a$ and $N\mu = d$. If further a (or d) contains a prime p in first power, which divides the discriminant of the cubic field, then $p = \mathfrak{p}^3$ if and only if b and c both are divisible by p. Otherwise $p = \mathfrak{p}^2 \cdot \mathfrak{p}_1$. Then (λ) (or (μ)) contains $\mathfrak{p}$ if b (or c) is divisible by p and contains $\mathfrak{p}_1$ if it is not.*

Proof. By (13) α cannot contain a higher power of a common prime ideal divisor than a and hence, since $N\alpha = a^2 d$, we have $Nj = a^2$, $N\lambda = a$ and $N\mu = d$. The further propositions of the lemma follows easily from Dedekind's theorem [1] that (p) is divisible by the square of a prime ideal if and only if the discriminant of the field is divisible by p.

Delaunay [4] gives further necessary conditions for the solubility of (2). He states two congruences (p. 259), which must both be satisfied. They are if and only if $a_2 b_3 - a_3 b_2$ is divisible by (a_1, b_1), where $\varepsilon = a_1 \alpha + b_1 \beta + c_1$ is the fundamental unit of $R(1, \alpha, \beta)$, $\lambda = a_2 \alpha + b_2 \beta + c_2$ and $\mu = a_3 \alpha + b_3 \beta + c_3$. If the congruences are identically satisfied he can decide, whether (2) is soluble or not (the number of solutions is either 2 or none). If the congruences are satisfied but not identically he shows that (2) must belong to $R(1, k_1 \alpha, k_1^2 \beta)$, a sub-ring of $R(1, \alpha, \beta)$ where α and β are defined by a certain form (a, b, c, d) among the equivalent forms (2) and k_1 is an integer > 1, and hence may be written $(a, b k_1, c k_1^2, d k_1^3) = 1$. This form may be examined in its ring as before, and so on. This is the 'Algorithmus der Erhöhung', which ends if either some of the necessary conditions fails or the congruences are identically satisfied. There are cases, however, where the algorithm doesn't end, and

Delaunay cannot solve the problem generally. We confine ourselves to this indication and refer to the cited paper. The only cases $kf^2 \leq 100$, where these further conditions are needed, is 63 which gives two forms (2) where the corresponding numbers λ and μ belong to the ring and 76 with one such form. The two congruences, however, are not satisfied for 63, if the calculated unit in each case really is fundamental.

To find the solutions of forms $(1, p, q, r) = 1$ belonging to the same cubic field we have to determine the fundamental units of the corresponding rings, which all are powers of the fundamental unit of the field. Then it is generally most advantageous to determine the fundamental ring of the field. The ring represented by a form $(a, b, kc, k^2 d)$ belongs to the ring represented by (ka, b, c, d) and with k^2 times less discriminant. To decide whether a ring $R(\theta)$ belongs to a ring $R(\varrho)$ we have by Nagell ([6] Satz XV):

Lemma 5. *A necessary and sufficient condition that a cubic integer θ belong to the ring $R(\varrho)$, where $D(\theta) = A^2 \cdot D(\varrho)$, is that*

$$\theta = \frac{a + b\varrho}{c + d\varrho}$$

where a, b, c and d are rational integers such that

$$N(c + d\varrho) = A = \pm(ad - bc) \text{ and } (c, d) / (a, b).$$

It is always possible but often very laborious to calculate the fundamental unit of a given ring (cp Berwick [1]). I proceed in this paper in a simple but rather unmethodical way which is successful in many cases. To find a unit we factorize integers of the ring, especially such the norms of which contain only powers of 2 or 3, and try to get the unit as a rational function of some of these integers. Next chapter gives many examples. Then it remains to decide whether the found unit is fundamental and in order to do that we use a method by Nagell (cp [7] p. 7). Suppose that we have determined the unit ε, $0 < \varepsilon < 1$, and that

$$\varepsilon = \eta^m = (u + v\varrho + w\varrho^2)^m$$

with $m \geq 2$. This gives

$$w = \pm \frac{1}{\sqrt{D(\varrho)}} \cdot [(\varrho'' - \varrho')\eta + (\varrho - \varrho'')\eta' + (\varrho' - \varrho)\eta'']$$

and we get an upper limit for $|w|$. We can always determine m_0 such that $w = 0$ if $m > m_0$. Hence we have to examine a finite number of cases with $w \neq 0$. If $w = 0$ we have

$$|D(\varepsilon)| \geq |D(\eta)| = |D(u + v\varrho)| = v^6 \cdot |D(\varrho)|$$

and this gives an upper limit for $|v|$. An inconveniance to this method is that this limit often will be very great even if we can show by congruences that only a fractional part of the number of values of v (or u) must be examined.

Having determined the fundamental unit ε we have to examine the condition

$$\varepsilon^n = x + y\theta. \tag{5}$$

Then we often use the following theorem:

Theorem 8. *Let ε be the fundamental unit of the ring $R(\theta)$, $0 < \varepsilon < 1$, and suppose*

$$\varepsilon = \eta^m, \quad m \geq 1.$$

Then the condition (5) may be written either

$$(\varphi + a)^{mn} = u + v\varphi \tag{14}$$

or

$$(\varphi + a)^{mn} = u + v\varphi^2 \tag{15}$$

where φ belongs to $R(\eta)$. Instead of (15) we can always, if suitable, get a condition of the type

$$(\varphi^2 + a)^{mn} = u + v\varphi \tag{16}$$

where φ belongs to $R(\theta)$.

Proof. It is easy to determine

$$k\theta = A\eta^2 + B\eta + C \tag{17}$$

where k, A, B and C are rational integers. If $A = 0$ the substitution

$$\eta = \varphi + a$$

gives (14), where u and v are rational integers, since φ must be the real root of an irreducible equation of the third degree. If $A \neq 0$, we make the substitution

$$\varphi = \frac{2A\eta + B}{d}, \quad \text{where } d = (2A, B).$$

Then (17) gives

$$4Ak\theta = d^2\varphi^2 + 4AC - B^2.$$

Further we put

$$\frac{2A}{d} \cdot \eta = \varphi - \frac{B}{d} = \varphi + a$$

and this gives (15), where u and v are rational integers, since φ is of the third degree. Instead of (17) we can write

$$k_1\eta = A_1\theta^2 + B_1\theta + C_1. \tag{17'}$$

Then $A \neq 0$ implies $A_1 \neq 0$. Now we substitute

$$\varphi = \frac{2A_1\theta + B_1}{d_1}$$

where $d_1 = 1$ if B_1 is odd and $d_1 = 2$ if B_1 is even. Then (17') gives

$$4A_1k_1\eta = d_1^2\varphi^2 + 4A_1C_1 - B_1^2 = d_1^2(\varphi^2 + a)$$

and this gives (16) with the same argumentation as before.

Conversely every integer solution (u, v) of (14), (15) or (16) corresponds to an integer solution (x, y) of (5), since ε belongs to $R(\theta)$ and is of the third degree. Then the theorem is completely proved.

Now put

$$\varphi^i = a_i\varphi^2 + b_i\varphi + c_i. \tag{18}$$

Then if not both $n<0$ and $|\varphi|$ (or $|\varphi^2|$)$>a$, the relations (14), (15) and (16) give respectively

$$\sum_{i=0}^{\infty} \binom{mn}{i} \cdot a^{mn-i} \cdot a_i = 0 \tag{14'}$$

$$\sum_{i=0}^{\infty} \binom{mn}{i} \cdot a^{mn-i} \cdot b_i = 0 \quad \text{and} \tag{15'}$$

$$\sum_{i=0}^{\infty} \binom{mn}{i} \cdot a^{mn-i} \cdot a_{2i} = 0. \tag{16'}$$

$n \geq 0$ gives sums with a finite number cf terms and $n<0$ gives convergent infinite series. If $(\varphi, p) \neq 1$ then, since $(\varphi, a) = 1$, a^{mn-i} must be a p-adic unit for all values of i whether n is positive or negative. Hence we often can show the impossibility of some of the three relations in a p-adic way irrespective of the sign of n. Since

the cubic field is real we have $|\varphi|$ (or $|\varphi^2|$) $\neq |a|$ and hence we can always get a convergent sum. If not both $n<0$ and $|\varphi|<|a|$ we can write

$$(\varphi+a)^{mn}=\sum_{i=0}^{\infty}\binom{mn}{i}\cdot\varphi^{mn-i}\cdot a_i.$$

In (14′) we can suppose $n\geq 0$, if $D(\varphi)\neq -23$, by

Lemma 6 (Nagell [3], Hilfssatz III). *If η is a unit, $D(\eta)<0$, $0<\eta<1$, then*

$$\eta^n=u+v\eta$$

implies that $n\geq 0$, except that $\eta^{-2}=1+\eta$ if $\eta^3=1-\eta^2$. In this case $D(\eta)=-23$.

Further we can generally find all the eventually solutions of (5) with $n<0$ by

Lemma 7. *A soluble irreducible form can always be written $F(u, v)=(1, p, q, r)=1$ with $p\leq 1$ and $r>0$. Suppose $D(F)<0$ and $0<\varepsilon<1$, where ε is the fundamental unit in the corresponding cubic ring. Then, if v_1 and $v_2>0$ and $D\left(1, p, q, r-\frac{1}{v_1^3}\right)$ and $D\left(1, p, q, r+\frac{1}{v_2^3}\right)<0$, a solution of (5) with $n<0$ implies $-v_2<v<v_1$. If specially $p=0$, $n<0$ implies that $0<v<3\cdot\sqrt[3]{\frac{2r}{|D(F)|}}$ (or, if $D(F)=-108k$, $0<v<\sqrt[3]{\frac{r}{2k}}$).*

Proof. Since $\theta>0$ is defined by $F(\theta, -1)=0$ we see that $uv<0$, if $v\leq -v_2$ or $v\geq v_1$. Then

$$(u+v\theta')\cdot(u+v\theta'')=u^2+(p-\theta)\cdot uv+\frac{r}{\theta}\cdot v^2>1,$$

$\left(\text{since } \frac{1}{\theta}-\left(\frac{1-\theta}{2}\right)^2>1, \text{ if } 0<\theta<1\right)$. Hence $\varepsilon^n=u+v\theta<1$, i.e. $n>0$. The special result for $p=0$ follows immediately from (6).

By (6) we see that if the unit η is defined by

$$\eta^3=p\eta^2-q\eta+1$$

then $D(\eta)$ even implies p and q both odd and hence, if we choose the arbitrary integer a odd in (14), we get a φ which satisfies the function congruence

$$\varphi^3\equiv 0 \pmod 2.$$

If further both p and q are divisible by 3, which generally is the fact, and if

$$\frac{2A}{d} = \frac{2B}{d} \pmod 3$$

in (17), we get a φ in (15) such that

$$\varphi^3 \equiv 0 \pmod 3.$$

Such a φ can always be determined in (14) too, which can be used if D is odd. Then we get in (14′) and (15′)

$$a_i \equiv 0 \left(\mathrm{mod}\ 2^{\left[\frac{i}{3}\right]}\right) \text{ and } b_i \equiv 0 \left(\mathrm{mod}\ 3^{\left[\frac{i}{3}\right]}\right)$$

and hence we can treat (14′) and (15′) in a p-adic way.

In other cases we may try different methods. If $|a|>1$ we often can write

$$\sum_{i=1}^{\infty} \binom{m\,n}{i} \cdot b_{mn-i} \cdot a^i = 0 \tag{15''}$$

and sometimes treat (15″) with regard to any prime p dividing a, since we then always have a period k such that $b_{i+k} \equiv b_i \pmod p$, whether i is positive or not. We can also give up making ε a binom and substitute $\theta = \varphi + c$ so that $\varphi^3 \equiv 0 \pmod p$, which gives

$$\varepsilon^n = (A\varphi^2 + B\varphi + C)^n = U + V\varphi.$$

Often congruence conditions for n obtained in different ways can be shown incompatible. Rather often we make use of a lemma by Delaunay (cp [4] p 264):

Lemma 8. *Let ε_1 be a unit in $R(\theta)$ and suppose that*

$$\varepsilon_1 = a_1 p \varphi^2 + b_1 p \varphi + c_1$$

where p is an odd prime, $\varphi = p^t \cdot \theta$, $t \geq 0$ and $p \nmid a_1$. Then no power ε_1^m (m positive or negative) can be a binom $A\theta + B$.

Proof. In $\varepsilon_1^m = (a_1 p \varphi^2 + b_1 p \varphi + c_1)^m$ we get as coefficient for φ^2 if $m > 0$

$$m \cdot c_1^{m-1} \cdot p \cdot a_1 + \sum_{i=2}^{m} \binom{m}{i} \cdot c_1^{m-i} \cdot p^i \cdot A_i$$

where A_i are rational integers. We easily see that every term in the sum must contain a higher power of p than the first term, if

$p > 2$, and hence the coefficient cannot be 0. Delaunay regards the case m positive but since $(c_1, p) = 1$, $\varepsilon_1 \cdot \varepsilon_1^{-1} = 1$ gives $\varepsilon_1^{-1} = a_1' \cdot p\varphi^2 + b_1' \cdot p\varphi + c_1'$, where $p \nmid a_1'$, and hence the lemma is proved even for $m < 0$.

If further ε_1 is the least power of the fundamental unit ε where the coefficients for θ^2 and θ are both divisible by p and if p is a divisor of $k = \frac{N(a\theta - b \quad aP)}{d^2}$, where $\varepsilon = a\theta^2 + b\theta + c$, $(a, b) = d$ and $\theta^3 = P\theta^2 - Q\theta + R$, then the relation $\varepsilon^n = u + v\theta$ is impossible if $n \neq 0$. This follows from

$$\varepsilon'^n - \varepsilon''^n = (\theta' - \theta'') \cdot v$$

i.e. v must be divisible by $\frac{\varepsilon' - \varepsilon''}{\theta' - \theta''} = -a\theta + b + aP$. If $P = 0$ we get $N(-a\theta + b) = b^3 + Qa^2 b - Ra^3 = F(b, -a)$, i.e. $k = \frac{F(b, -a)}{d^2}$. The divisors of k, however, are often very great. Delaunay ([4] p 265) gives complicated conditions to decide, whether such a divisor satisfies lemma 8, but I have made no use of them.

Finally we need the following simple lemma:

Lemma 9. *The binomial coefficient* $\binom{n}{p^q + r}$, *where* $0 < r < p^q$, *is divisible by at least the same power of the prime* p *as* $\binom{n}{p^q}$. *Specially, if* p, n *and* $p^{-}r$, $\binom{n}{p^q : r}$ *contains a higher power of* p *than* $\binom{n}{p^q}$.

Proof. $\binom{n}{p^q + r} = \binom{n}{p^q} \cdot \frac{(n - p^q)(n \quad p^q - 1) \cdot \quad \cdot (n \quad p^q - r + 1)}{(p^q + 1)(p^q + 2) \cdot \cdots \cdot (p^q + r)}$ and since $\frac{\prod_{i=1}^{r} (p^q + i)}{r!}$ is an integer not divisible by p, $\binom{n}{p^q + r}$ and $\binom{n}{p^q} \cdot \binom{n - p^q}{r}$ are divisible by exactly the same power of p. This proves the lemma.

II

Applications to the equations $y^2 - kf^2 = x^3$

1. The equations $y^2 - f^2 = x^3$

The case $f = 1$ was at first solved by Euler. $f = 2, 4, 5$ and 7 are also treated and give only the trivial solution $(0, \pm f)$. Nagell has solved the case $f = 3$ [7]. I shall give the solutions in the cases $f = 6, 8, 9$ and 10.

$f = 6$, i.e. *the equations* $y^2 - 36 = x^3$. By theorem 2 we get five forms:

(1) $$u^3 + v^3 = 12$$

(2) $$U^3 + 2V^3 = 6, \text{ i.e. } 4u^3 + v^3 = 3, \qquad x = -4uv$$

(3) $$u^3 + 3v^3 = 4 \qquad x = -3uv$$

(4) $$U^3 + 6V^3 = 2, \text{ i.e. } 4u^3 + 3v^3 = 1, \qquad x = -12uv$$

(5) $$2U^3 + 3V^3 = 2, \text{ i.e. } u^3 + 12v^3 = 1, \qquad x = -12uv.$$

(1) is impossible modulo 9 and hence insoluble.

(2) has by theorem 3 the only solution $u = 1$, $v = -1$, corresponding to $x = 4$.

(3) belongs to the field $K(\sqrt[3]{3})$. Put $\sqrt[3]{3} = \theta$. Then the fundamental unit of the field is $\theta^2 - 2$ and we get

(6) $$u + v\theta = (\theta - 1)^2 \cdot (\theta^2 - 2)^n.$$

The solution $(1, 1)$ of (3) corresponds to $n = -1$. If there are more solutions, u and v must have opposite signs and hence, if $n \neq -1$

$$0 < u + v\theta = \frac{4}{u^2 - uv\theta + v^2\theta^2} < 1.$$

Since $\theta - 1 > \frac{3}{10}$ we get $(\theta^2 - 2)^n < \frac{100}{9} < (\theta^2 - 2)^{-1}$ and we must have $n > 0$. From (6) we get

(6′)
$$\sum_{i=0}\left[\binom{n}{3i}\cdot(-2)^{n-3i}+\binom{n}{3i-1}\cdot(-2)^{n-3i-1}\right]\cdot 3^{2i} = 6\sum_{i=0}\binom{n}{3i-2}\cdot(-2)^{n-3i-2}\cdot 3^{2i}$$

which at once gives the necessary condition

$$n \equiv -1 \pmod 3.$$

Suppose $n \equiv -1 \pmod{3^p}$. Then (6′) gives

$$(-2)^n + n(-2)^{n-1} + \sum_{i=1}(-1)^n(2^{n-3i}+2^{n-3i-1})\cdot 3^{2i} \equiv -\sum_{i=0}(-1)^n\cdot 2^{n-3i-1}\cdot 3^{2i+1} \pmod{3^{p+1}}$$

i.e.

$$(n+1)\cdot 2^{n-1} \equiv 0 \pmod{3^{p+1}}$$

and

$$n \equiv -1 \pmod{3^{p+1}}.$$

Then $n = -1$ gives the only solution, which corresponds to $x = -3$.

(4) has by theorem 3 the only solution $(1, -1)$, corresponding to $x = 12$.

(5) has only the solution $(1, 0)$ by the last part of theorem 3, since the equation $2u^3 + 3v^3 = 1$, which belongs to the same field, has the solution $(-1, 1)$. Hence the Diophantine equation

$$y^2 - 36 = x^3$$

has exactly the four integer solutions

$$\begin{aligned} x &= -3 & y &= \pm 3 \\ x &= 0 & y &= \pm 6 \\ x &= 4 & y &= \pm 10 \\ x &= 12 & y &= \pm 42. \end{aligned}$$

$f = 8$, i.e. *the equation* $y^2 - 64 = x^3$. By theorem 2 we get two forms:

(7) $$u^3 + v^3 = 16 \qquad x = -uv$$

and

(8) $$U^3 + 2V^3 = 8, \text{ i.e. } u^3 + 2v^3 = 1, \quad x = -8uv.$$

(7) has the only solution $(2, 2)$ corresponding to $x = -4$.

(8) has by theorem 3 only the two solutions $(1, 0)$ and $(-1, 1)$, corresponding to $x = 0$ and 8 resp.

The three solutions can also be derived immediately, since $64 = 2^6$. Then we have the solution $(4x, 8y)$, if (x, y) is a solution of $y^2 - 1 = x^3$. Hence the Diophantine equation

$$y^2 - 64 = x^3$$

has exactly the three integer solutions

$$\begin{aligned} x &= -4 & y &= 0 \\ x &= 0 & y &= \pm 8 \\ x &= 8 & y &= \pm 24. \end{aligned}$$

$f = 9$, i.e. *the equation* $y^2 - 81 = x^3$. By theorem 2 we get five forms:

$$u^3 + v^3 = 18 \tag{9}$$

$$u^3 + 2v^3 = 9 \tag{10}$$

$$U^3 + 3V^3 = 6, \quad \text{i.e.} \quad 9u^3 + v^3 = 2 \tag{11}$$

$$U^3 + 6V^3 = 3, \quad \text{i.e.} \quad 9u^3 + 2v^3 = 1 \tag{12}$$

$$2U^3 + 3V^3 = 3, \quad \text{i.e.} \quad 18u^3 + v^3 = 1, \quad x = -18uv. \tag{13}$$

(9) is impossible modulo 7 and (10), (11) and (12) are impossible modulo 9.

(13) has only the solution (0, 1), since the equation $2u^3 + 3v^3 = 1$ belongs to the same field and has the solution $(-1, 1)$ (theorem 3, last part).

Hence the Diophantine equation

$$y^2 - 81 = x^3$$

has exactly one integer solution

$$x = 0 \qquad y = \pm 9.$$

$f = 10$, i.e. *the equation* $y^2 - 100 = x^3$. By theorem 2 we get five forms:

$$u^3 + v^3 = 20 \tag{14}$$

$$U^3 + 2V^3 = 10, \quad \text{i.e.} \quad 4u^3 + v^3 = 5, \qquad x = -4uv \tag{15}$$

$$u^3 + 5v^3 = 4 \qquad x = -5uv \tag{16}$$

$$U^3 + 10V^3 = 2, \quad \text{i.e.} \quad 4u^3 + 5v^3 = 1, \qquad x = -20uv \tag{17}$$

$$2U^3 + 5V^3 = 2, \quad \text{i.e.} \quad u^3 + 20v^3 = 1, \qquad x = -20uv. \tag{18}$$

(14) can easily be shown insoluble.

(15) has the solutions (1, 1) and (2, −3). We make the substitution $u = a - b$, $v = a + 4b$, which gives

$$a^3 + 12ab^2 + 12b^3 = 1. \tag{19}$$

(19) must contain all the solutions of (15) and corresponds to the ring $R(\theta)$, defined by

$$\theta^3 + 12\theta - 12 = 0 \tag{20}$$

with the fundamental unit $\varepsilon = 1 - \theta$, where

$$\varepsilon^3 - 3\varepsilon^2 - 15\varepsilon - 1 = 0.$$

ε is moreover the square of $\sqrt[3]{2} - 1$, the fundamental unit of the ring $R(\sqrt[3]{2})$. Then we have the condition

$$(1 - \theta)^n = a + b\theta$$

where the two known solutions correspond to $n = 0$ and 1. By lemma 6 a third solution must have $n > 1$ and with the notation $\theta^i = a_i\theta^2 + b_i\theta + c_i$ (I, 18) we get

$$\sum_{i=2}^{n} (-1)^i \cdot \binom{n}{i} \cdot a_i = 0.$$

Put $n = 2^p \cdot n_1 + \lambda$, n_1 odd, $\lambda = 0$ or 1, and $i = 2^q + k$, $0 \leq k < 2^q$. Then, since $\theta^3 \equiv 0 \pmod{2^2}$, we get

$$\binom{n}{i} \cdot a_i \equiv 0 \left(\mathrm{mod}\ 2^{p-q+2\cdot\left[\frac{i}{3}\right]}\right)$$

and since $i > 2$ gives $q \leq {}^2\log i \leq 2 \cdot \left[\frac{i}{3}\right]$, we get

$$\sum_{i=2}^{n} (-1)^i \cdot \binom{n}{i} \cdot a_i \equiv 2^{p-1} \pmod{2^p}$$

and there are only solutions for $n = 0$ and 1, corresponding to $x = -4$ and 24 respectively.

(16) belongs to the field $K(\sqrt[3]{5})$, which has the fundamental unit $\varepsilon = 2\varrho^2 - 4\varrho + 1$, with $\varrho = \sqrt[3]{5}$. Then we get

$$u + v\varrho = (\varrho - 1) \cdot (2\varrho^2 - 4\varrho + 1)^n.$$

Put $\varphi = \varrho - 1$. This gives

$$u - v - v\varphi = \varphi \cdot (2\varphi^2 - 1)^n \tag{21}$$

where

$$\varphi^3 = -3\varphi^2 - 3\varphi + 4.$$

With the notations in (I, 18) the relation (21) gives

$$\sum_{i=1} (-1)^i \cdot \binom{n}{i} \cdot 2^i \cdot (b_{2i} - 3a_{2i}) = 0. \tag{21'}$$

Put $n = 2^p \cdot n_1 + \lambda$, n_1 odd, $\lambda = 0$ or 1, and $i = 2^q + k$, $0 \leq k < 2^q$. Then, if $i > 4$

$$\binom{n}{i} \cdot 2^i \equiv 0 \pmod{2^{p-q+i}} \text{ i.e. } \equiv 0 \pmod{2^{p+3}}.$$

$b_{2i} - 3a_{2i} = -3, -5$ and 94 for $i = 1, 2$ and 3 resp. and is odd for $i = 4$. This gives at first

$$6n - 10n \cdot (n-1) \equiv -10n^2 \equiv 0 \pmod{2^4}$$

i.e. $n \equiv 0 \pmod 4$, and further

$$-10n^2 \equiv 2^{p+2} \pmod{2^{p+3}}$$

which is impossible, since $2p + 1 > p + 2$, if $p \geq 2$. As for $u^3 + 3v^3 = 4$ in the case $f = 6$ we see that $n \geq 0$ and then (21) has only the solution $n = 0$, corresponding to $x = 5$.

(17) has by theorem 3 no solutions but $(-1, 1)$, which corresponds to $x = 20$.

(18) has by the same theorem the two solutions $(1, 0)$ and $(-19, 7)$, corresponding to $x = 0$ and 2660.

Hence the Diophantine equation

$$y^2 - 100 = x^3$$

has exactly the six integer solutions

$$\begin{array}{ll} x = -4 & y = \pm 6 \\ x = 0 & y = \pm 10 \\ x = 5 & y = \pm 15 \\ x = 20 & y = \pm 90 \\ x = 24 & y = \pm 118 \\ x = 2660 & y = \pm 137190. \end{array}$$

2. The equations $y^2 - 2f^2 = x^3$

The case $f = 1$ was solved by Delaunay ([4] 13, p. 265) and by A. Brauer [1]. We get the form $(1, 0, 3, 2) = 1$, corresponding to the ring $R(\varrho)$, where

$$\varrho^3 = -3\varrho + 2. \tag{1}$$

This ring is fundamental and it has the fundamental unit $\varepsilon = -\varrho^2 - \varrho + 1$, where

$$\varepsilon^3 = 9\varepsilon^2 - 21\varepsilon + 1. \tag{2}$$

By theorem 4 we see that the cases $f = 2, 3, 5$ and 6 have all their solutions included in either the reducible form $3a^2b + 2b^3 = f$ or the irreducible form $(1, 0, 3, 2) = f$. All forms $G = 1$, derived from this later form, correspond to rings belonging to $R(\varrho)$. $f = 4$ gives no integer solution. 7 divides into two different prime ideals in the field $K(\sqrt{2})$, and we shall see that we get forms belonging to different fields in the case $f = 7$. We shall treat the cases $f = 2, 3, 5, 6$ and 7.

$f = 2$, i.e. *the equation* $y^2 - 8 = x^3$. By theorem 4 we have to examine the reducible form $3a^2b + 2b^3 = 2$ with the solution $(0, 1)$, corresponding to $x = -2$, and

$$\pm y + 2\sqrt{2} = (1 + \sqrt{2}) \cdot (a + b\sqrt{2})^3$$

which gives

$$a^3 - 3a^2b - 6ab^2 + 2b^3 = 2.$$

The substitution $a = 2v$, $b = u - 2v$ gives

$$u^3 - 6uv^2 + 8v^3 = 1 \tag{3}$$

and the substitution $a = u_1 + v_1$, $b = -u_1 + v_1$ gives

$$u_1^3 - 3u_1v_1^2 + 6v_1^3 = 1. \tag{4}$$

(3) corresponds to the ring $R(\theta)$, where θ is the real root of

$$\theta^3 = 6\theta + 8. \tag{5}$$

$R(\theta)$ has the fundamental unit $\varepsilon = 3 - \theta$ which is just the ε defined by (2).

(4) corresponds to the ring $R(\theta_1)$ defined by

$$\theta_1^3 = 3\theta_1 + 6. \tag{6}$$

From the substitutions we get $\theta = \dfrac{4}{\theta_1 - 1} = \dfrac{\theta_1^2}{2} + \dfrac{\theta_1}{2} - 1$. Then $\varepsilon = 3 - \theta = 4 - \dfrac{\theta_1}{2} - \dfrac{\theta_1^2}{2}$ does not belong to $R(\theta_1)$, but

$$\varepsilon^2 = 19 - \theta_1 - 3\,\theta_1^2$$

is the fundamental unit of $R(\theta_1)$.

To decide, whether (3) has a third solution, we have to examine

$$\varepsilon^n = (3 - \theta)^n = u + v\,\theta. \tag{7}$$

$n = 0$ and 1 give the known solutions (1, 0) and (3, −1), corresponding to $x = 2$ and 46 respectively.

Further we get $\theta_1 = 1 + \dfrac{4}{\theta} = \dfrac{\theta^2}{2} - 2$ and then by theorem 8 the condition $(\varepsilon^2)^n = u_1 + v_1\,\theta_1$ may be replaced by

$$(3 - \theta)^{2n} = U + V\,\theta^2 \tag{8}$$

where $n = 0$, i.e. the solution (1, 0), corresponds to $x = 1$. Then the solution of (4) is equivalent to the solution of (8).

By (I, 18) we write

$$\theta^i = a_i\,\theta^2 + b_i\,\theta + c_i.$$

For the examination of (7) and (8) we use the following lemma:

Lemma 10. *We have always*

$$a_{i+1} = b_i$$

and if $r > 0$ *we get*

$$b_{2^r+1} \equiv 2^r \pmod{2^{r+1}}$$

if $r = 1$ *or* 2, *and otherwise*

$$b_{2^r+k} \equiv 0 \pmod{2^{r+1}} \quad 0 \leq k < 2^r.$$

Proof. $a_{i+1} = b_i$ follows immediately from $a_3 = 0$. It is easy to control that from

$$\theta^p = 2^q\,(a'\,\theta^2 + 4\,b'\,\theta + 32\,c')$$

with a', b' and c' odd integers, follows

$$\theta^{2p} = 2^{2q+1}\,(a''\,\theta^2 + 4\,b''\,\theta + 32\,c'')$$

with a'', b'' and c'' odd integers. Now this condition is satisfied by $p = 8$, $q = 3$, and then we get the recursion formula

(9) $$\theta^{2^r} = 2^{2^{r-1}-1}(a\,\theta^2 + 4b\,\theta + 32c)$$

where a, b and c are odd integers and $r \geq 3$. If b and c are allowed to be 0, the formula is satisfied even by $r = 1$ and 2. Hence, if $r > 3$, we always have the function congruence

$$\theta^{2^r+k} \equiv 0 \pmod{2^{r+1}}$$

and for the coefficient b_{2^r+k} this congruence is satisfied even if $r = 3$. An examination of the remaining case $r = 1$ or 2 gives the result of the lemma.

A. Examination of (7). By lemma 6 and since $n = 0$ and 1 correspond to the known solutions, we can suppose $n > 1$. (7) is equivalent to

(7′) $$\sum_{i=2}^{n} (-1)^i \binom{n}{i} \cdot 3^{n-i} \cdot a_i = 0.$$

Since $a_2 = 1$ and $a_i \equiv 0 \pmod 2$, if $i > 2$, (7′) gives the condition

$$\binom{n}{2} \equiv 0 \pmod 2$$

i.e. $n \equiv 0$ or $1 \pmod 4$. For brevity we write

$$u_i \quad (-1)^i \binom{n}{i} \cdot 3^{n-i} \cdot a_i.$$

I. $n = 2^p \cdot q$, $p \geq 2$, q odd.

We distinguish the cases $p = 2$ and $p \geq 3$.

a) $p = 2$. Then

$$u_2 \equiv u_4 \equiv 2 \pmod 4$$

and otherwise, according to (9)

$$u_i \equiv 0 \pmod 8.$$

Hence we get the necessary condition for (7′)

$$u_2 + u_4 \equiv 0 \pmod 8$$

i.e.

$$3 \cdot \binom{n}{2} + 2 \cdot \binom{n}{4} \equiv 0 \pmod 8.$$

But this implies

$$q \equiv 0 \pmod 2$$

which contradicts the supposition.

b) $p \geq 3$. Then

$$u_2 \equiv u_4 \equiv 2^{p-1} \pmod{2^p}$$

and

$$u_8 \equiv 2^p \pmod{2^{p+1}}$$

while otherwise

$$u_i \equiv 0 \pmod{2^{p+1}}.$$

Hence we have the necessary condition

$$u_2 + u_4 \equiv 2^p \pmod{2^{p+1}}$$

which leads to a contradiction. Then $n+0$ cannot be even.

II. $n = 2^p \cdot q + 1$, $p \geq 2$, q odd.

Let $\lambda(x)$ be the exponent of the highest power of 2 which divides x, i.e.

$$x = x' \cdot 2^{\lambda(x)}, \quad x' \text{ odd}.$$

Then, since the prime is 2, we get in a sequence of terms u_i

$$\lambda(\Sigma u_i) = \text{Min } \lambda(u_i)$$

if the number of terms with the lowest value of λ is odd, and

$$\lambda(\Sigma u_i) > \text{Min } \lambda(u_i)$$

if this number is even. Then if $\lambda(u_i)$ increases (or ev. decreases) rapidly and regularly enough with increasing i, we can successively put up new necessary conditions for (7'). We get the following table:

i	a_i	$\lambda(u_i)$	
		$p=2$	$p \geq 3$
2	1	1	$p-1$
4	6	1	$p-1$
5	8	3	$p+1$
6	$2^2 3^2$	$r+1$	$p+1$
8	$2^3 \cdot 35$	r	p

The table gives the lowest values of $\lambda(u_i)$. For all the other values of i we have $\lambda(u_i) > r+1$ and $p+1$ resp. If $p=2$ we put $n = 5 + 2^r q_1$, q_1 odd and hence $r \geq 3$.

a) $p=2$. We have

$$n = 4q + 1$$

and further we put

$$n \equiv 5 + 2^r \pmod{2^{r+1}}.$$

Then $r = 3$ corresponds to

$$q \equiv -1 \pmod 4$$

and $r > 3$ corresponds to

$$q \equiv 1 \pmod 4.$$

If $r = 3$, the first necessary condition

$$u_2 + u_4 \equiv 0 \pmod{2^4}$$

is satisfied, but the next condition

$$u_2 + u_4 \not\equiv u_5 + u_8 \pmod{2^5}$$

gives the contradiction, for if $q \equiv -1 \pmod 4$, the congruence is satisfied. Since $a_8 = 2^3 \cdot 35 = 2^3 \cdot 3^3 + 2^6$, we can put $a_8 = 2^3 \cdot 3^3$ by calculation of u_8, when the modulus is at most 2^{r+3} or 2^{p+3} resp. If $r > 3$ the first condition

$$u_2 + u_4 \equiv 2^3 \pmod{2^4}$$

is also satisfied. The next condition

$$u_2 + u_4 + u_5 \equiv 0 \pmod{2^r}$$

gives, since $n \equiv 5 \pmod{2^r}$

$$\binom{5}{2} \cdot 3^3 + \binom{5}{4} \cdot 2 \cdot 3^2 - 8 \equiv 0 \pmod{2^r}$$

i.e.

$$352 = 11 \cdot 2^5 \equiv 0 \pmod{2^r}$$

and hence we only can have

$$r = 4 \text{ or } 5.$$

Then we have the condition

$$u_2 + u_4 + u_5 \equiv 2^r \pmod{2^{r+1}}$$

and, since $n \equiv 5 + 2^r \pmod{2^{r+1}}$, this gives

$$176 + 135 \cdot 2^{r-2} \equiv 2^{r-1} \pmod{2^r}$$

but this is not satisfied if $r = 4$ or 5, because 176 is divisible by 2^4.

b) $p \geq 3$. Here the table gives the two first necessary conditions

$$u_2 + u_4 \equiv 2^p \pmod{2^{p+1}}$$

and

$$u_2 + u_4 + u_8 \equiv 0 \pmod{2^{p+2}}.$$

The first condition is satisfied but the other one gives the contradiction, which is easily seen modulo 8 after division by $n \cdot q \cdot 3^{n-5} \cdot 2^{p-1}$. Then (7) has only the two solutions $n = 0$ and 1.

B. Examination of (8). Suppose

$$2n = 2^p \cdot q, \quad q \text{ odd}.$$

Then, if $i \geq 2$, we have by the lemmas 9 and 10

$$\binom{2n}{i} \cdot b_i \equiv 0 \pmod{2^{p+1}}$$

and hence

$$\sum_{i=1}^{\infty} (-1)^i \binom{2n}{i} \cdot 3^{2n-i} b_i = -2n \cdot 3^{2n-1} = 2^p \pmod{2^{p+1}}.$$

Then the equation

$$\sum_{i=1}^{\infty} (-1)^i \binom{2n}{i} \cdot 3^{2n-i} b_i = 0 \tag{8'}$$

which is equivalent to (8), cannot be satisfied, if $n \neq 0$. The discussion above is applicable even to the case $n < 0$, and hence (8) has only the solution $n = 0$.

Then the Diophantine equation

$$y^2 - 8 = x^3$$

has exactly the four integer solutions

$$\begin{aligned} x &= -2, & y &= 0 \\ x &= 1, & y &= \pm 3 \\ x &= 2, & y &= \pm 4 \\ x &= 46, & y &= \pm 312. \end{aligned}$$

$f = 3$, i.e. *the equation* $y^2 - 18 = x^3$. Since 3 is a prime of the second degree in $K(\sqrt{2})$, we get by theorem 4

$$\pm y + 3\sqrt{2} = \eta (a + b\sqrt{2})^3.$$

$\eta = 1$ gives no integer solution and $\eta = \varepsilon = 1 + \sqrt{2}$ gives the form

$$a^3 + 3a^2 b + 6ab^2 + 2b^3 = 3.$$

By theorem 6 this gives only one form $G=1$. The substitution $a=u+v,\ b=-2u-5v$ gives

$$u^3-21uv^2-38v^3=1. \tag{10}$$

The corresponding ring $R(\theta)$, defined by

$$\theta^3=21\theta-38 \tag{11}$$

belongs to the ring $R(\varrho)$, defined by (1), and by lemma 5 we determine

$$\theta=\frac{5\varrho-4}{2\varrho-1} \quad \text{and hence} \quad \varrho=\frac{\theta-4}{2\theta-5}$$

i.e.

$$\varrho=\frac{1}{3}(2\theta^2-5\theta-28).$$

Then we have the fundamental unit of $R(\varrho)$

$$\varepsilon=-\varrho^2-\varrho+1=-\frac{1}{3}(\theta^2+\theta-23).$$

Further we get

$$\varepsilon^2=-\frac{1}{3}(8\theta^2+14\theta-151)$$

and

$$\varepsilon^3=-17\theta^2-35\theta+293.$$

Then ε^3 is the fundamental unit of $R(\theta)$. By theorem 8 we now determine

$$2\theta=-\varepsilon^2+8\varepsilon-11$$

and hence the substitution

$$\varphi=\varepsilon-4$$

make it possible to substitute the condition $(\varepsilon^3)^n=u+v\theta$ by

$$(4+\varphi)^{3n}=U+V\varphi^2 \tag{12}$$

where

$$\varphi^3-3\varphi^2+3\varphi+3=0.$$

Then with the notions of (I, 18) we have to examine the condition

$$\sum_{i=1}^{\infty}\binom{3n}{i}\cdot b_i=0. \tag{12'}$$

Put $n=3^p n_1$, where $n_1 \not\equiv 0 \pmod 3$, and $i=3^q+r$, $0 \leq r < 3^q$. Since $b_i \equiv 0 \left(\mathrm{mod}\ 3^{\left[\frac{i}{3}\right]}\right)$ we get by lemma 9

$$\binom{3n}{i} \cdot b_i = 0 \left(\mathrm{mod}\ 3^{p+1-q+\left[\frac{i}{3}\right]+t}\right)$$

where $t=1$, if r is not divisible by 3 and $t=0$ in other cases. This shows immediately that

$$\binom{3n}{i} \cdot b_i \equiv 0 \pmod{3^{p+2}}$$

if $i \geq 4$ and we get the condition

$$3n + \binom{3n}{3} \cdot b_3 \equiv 0 \pmod{3^{p+2}}$$

which gives a contradiction. The argumentation is still valid, if $n<0$ and hence the Diophantine equation

$$y^2 - 18 = x^3$$

has the only integer solution

$$x=7, \quad y = \pm 19.$$

$f=5$, i.e. *the equation* $y^2-50=x^3$. Since 5 is a prime of the second degree in $K(\sqrt{2})$, we get by theorem 4

$$\pm y + 5\sqrt{2} = \eta (a+b\sqrt{2})^3.$$

$\eta=1$ gives

$$3a^2b + 2b^3 = 5$$

with the only solution $a=b=1$, corresponding to $x=-1$. $\eta=1+\sqrt{2}$ gives $a^3+3a^2b+6ab^2+2b^3=5$ or with $a=u+v$, $b=-v$

$$u^3 + 3uv^2 + 2v^3 = 5. \tag{13}$$

We must have $v \not\equiv 0 \pmod 5$ and since the congruence $u^3+3u+2 \equiv 0 \pmod 5$ is impossible, (13) can have no integer solutions. Hence the Diophantine equation

$$y^2 - 50 = x^3$$

has the only integer solution

$$x=-1 \quad y = \pm 7.$$

$f=6$, i.e. *the equation* $y^2-72=x^3$. By theorem 4 all the solutions are given by

$$y+6\sqrt{2}=\eta(a+b\sqrt{2})^3,\quad x=N(\eta)\cdot(a^2-2b^2).$$

$\eta=1$ gives no integer solution.

$\eta=1+\sqrt{2}$ gives as before after the substitution $a=u+v$, $b=-v$

$$u^3+3uv^2+2v^3=6. \tag{14}$$

By theorem 6 this can give at most 2 forms $G=1$. Now the substitution $u=u_1+4v_1$ $v=u_1-2v_1$ gives

$$u_1^3+6u_1v_1^2+16v_1^3=1 \tag{15}$$

and the substitution $u=2u_2$ $v=-u_2+3v_2$ gives

$$2u_2^3-3u_2^2v_2+9v_2^3=1. \tag{16}$$

(15) corresponds to the ring $R(\theta)$ defined by

$$\theta^3+6\theta-16=0 \tag{17}$$

and $R(\theta)$ belongs to the ring $R(\varrho)$ defined by (1). We get by lemma 5

$$\theta=\frac{4-2\varrho}{1+\varrho}=\varrho^2-\varrho+2.$$

Then

$$\varrho\quad\begin{matrix}4-\theta & 1\\ 2-\theta & 6\end{matrix}(\theta^2-2\theta+4)$$

and hence

$$\varepsilon=-\varrho^2-\varrho+1=\frac{1}{3}(-\theta^2-\theta+5)$$

where ε, defined by (2), is the fundamental unit of $R(\varrho)$. We get

$$\varepsilon^3=-8\theta^2+\theta+23$$

as the fundamental unit of $R(\theta)$. Since

$$\theta=\varepsilon^2-5\varepsilon+2$$

theorem 8 proposes the substitution $\varphi=2\varepsilon-5$ and we get the condition

$$(\varphi+5)^{3n}=U+V\varphi^2 \tag{18}$$

where

$$\varphi^3=3\cdot(\varphi^2+7\varphi-29).$$

Then by the notions of (I, 18) we hawe

$$\sum_{i=1}^{\infty} \binom{3n}{i} \cdot 5^{3n-i} \cdot b_i = 0. \tag{18'}$$

Put $n = 3^p \cdot n_1$, $n_1 \not\equiv 0 \pmod 3$. Then, exactly as in the case $y^2 - 18 = x^3$,

$$3n \cdot 25 + \binom{3n}{3} \cdot 21 = 0 \pmod{3^{p+2}}$$

which is not satisfied if $n \neq 0$. The argumentation is still valid if $n < 0$. $n = 0$ corresponds to $x = -2$.

(16) corresponds to the ring $R(1, \alpha, \beta)$, where

$$\begin{aligned} &\alpha^3 + 3\alpha^2 - 36 = 0 \\ &\beta^3 - 27\beta - 162 = 0 \\ &\alpha\beta = 18. \end{aligned} \tag{19}$$

$\beta = 3\gamma$ gives

$$\gamma^3 - 3\gamma - 6 = 0 \tag{6}$$

defining a ring which we have met and discussed in the case $y^2 - 8 = x^3$. Then $\alpha = \frac{6}{\gamma} = \gamma^2 - 3$ and $R(1, \alpha, \beta) = R(1, 3\gamma, \gamma^2)$. Moreover the fundamental unit (which we don't need here) is $\varepsilon^6 = 7447 + 1749\gamma - -2085\gamma^2 = 1192 - 2085\alpha + 583\beta$. Applying lemma 4 to $(2, -3, 0, 9) = 1$ we get $\gamma = \mathfrak{p}_1$, where $2 = \mathfrak{p}^2 \cdot \mathfrak{p}_1$. Now $(\gamma - 2) = \mathfrak{p}_1^2$ but this is no principle ideal of $R(1, 3\gamma, \gamma^2)$, much less $\mathfrak{p}_1 = \left(\frac{\gamma^2}{2} - \frac{\gamma}{2} - 1\right)$. Then (16 is insoluble. Hence the Diophantine equation

$$y^2 - 72 \quad x^3$$

has the only integer solution

$$x = -2, \quad y = \pm 8.$$

$f = 7$, i.e. *the equation* $y^2 - 98 = x^3$. Since $7 = (3 + \sqrt{2}) \cdot (3 - \sqrt{2})$ in the field $K\sqrt{2})$ we get by theorem 5

$$\pm y + 7\sqrt{2} = \eta \cdot (a + b\sqrt{2})^3 \quad \eta = 1 \text{ or } \varepsilon \tag{20}$$

and

$$\pm \frac{y}{7} + \sqrt{2} = \eta \cdot (3 + \sqrt{2}) \cdot (a + b\sqrt{2})^3 \quad \eta = 1, \ \varepsilon \text{ or } \varepsilon'. \tag{21}$$

$\eta=1$ in (20) gives a form without solutions. $\eta=1+\sqrt{2}$ gives

$$a^3+3a^2b+6ab^2+2b^3=7. \tag{20'}$$

This form has no solutions, since $b\equiv 0 \pmod 7$ and $a^3+3a^2-a+2\equiv 0 \pmod 7$.

The three equations (21) give forms corresponding to three other fields. $\eta=\sqrt{2}+1$ and $\sqrt{2}-1$ give respectively

$$4a^3+15a^2b+24ab^2+10b^3=1$$

and

$$2a^3-3a^2b+12ab^2-2b^3=1$$

which both can be shown insoluble modulo 7. $\eta=1$ gives

$$a^3+9a^2b+6ab^2+6b^3=1 \tag{21'}$$

or by the substitution $a=u-3v$, $b=v$

$$u^3-21uv^2-42v^3=1.$$

The corresponding ring $R(\theta)$ defined by

$$\theta^3=21\theta+42 \tag{22}$$

cannot belong to $R(\varrho)$, defined by (1), since the necessary condition of lemma 5, $c^3+3cd^2+2d^3=7$, is impossible with rational integers c and d. $R(\theta)$ is the fundamental ring of $K(\theta)$. In this field we have the factorizations $(2)=\mathfrak{p}^2\cdot\mathfrak{p}_1$, $(3)=\mathfrak{q}^3$, $(\theta+2)=\mathfrak{p}_1^3$ and $(\theta+3)=\mathfrak{p}\cdot\mathfrak{q}$ and then

$$\varepsilon\cdot(\theta+3)^6\cdot(\theta+2)=72$$

gives the unit $\varepsilon=3\theta^2+15\theta-167$, defined by

$$\varepsilon^3+375\varepsilon^2+35157\varepsilon-1=0. \tag{23}$$

Suppose

$$\varepsilon=\eta^m=(w\theta^2+v\theta+u)^m=3\theta^2+15\theta-167.$$

$m=2$ is impossible modulo 2. If $m>2$, the method by Nagell mentioned in chapter I gives $w=0$ and $|v|<7$, which is not satisfied. Then ε is the fundamental unit of $K(\theta)$ and by lemma 8 (21') has only the solution (1, 0). Hence the Diophantine equation

$$y^2-98=x^3$$

has exactly one integer solution

$$x=7, \quad y=\pm 21.$$

The first case, where further fields can appear, is $f=17$.

3. The equations $y^2-3f^2=x^3$

Delaunay has given the solution of the case $f=1$ [6]. This problem leads to the form $(1, 0, -3, 4)=1$, which corresponds to the ring $R(\varrho)$, defined by

$$\varrho^3=3\varrho+4. \tag{1}$$

$R(\varrho)$ is a fundamental ring and it has the fundamental unit $\varepsilon=\varrho^2+\varrho-7$, where ε is defined by

$$\varepsilon^3+15\varepsilon^2+57\varepsilon-1=0. \tag{2}$$

Since $k=3$, there can be no solution of the reducible form $3a^2b+kb^3=f$, if f is not divisible by 3. In the case $f=3$ there is only such a trivial solution and $f=5$ gives an insoluble equation. We shall here treat the remaining cases $f=2$, 4 and 6, which by theorem 4, except the 'trivial' solution $(-2, \pm 10)$ for $f=6$, have all their solutions contained in the form $(1, 0, -3, 4)=f$.

$f=2$, i.e. *the equation* $y^2-12=x^3$. Then we only have to examine

$$\pm y+2\sqrt{3}=(2+\sqrt{3})\cdot(a+b\sqrt{3})^3.$$

This gives

$$a^3-6a^2b+9ab^2+6b^3=2$$

from which at most two non-equivalent forms $G=1$ can be derived. The substitution $a=-u+2v$, $b=u$ gives

$$u^3+6uv^2+4v^3=1 \tag{3}$$

and the substitution $a=-4u+6v$, $b=u-v$ gives

$$u^3+6u^2v-27uv^2+24v^3=1. \tag{4}$$

(3) corresponds to the ring $R(\theta)$, defined by

$$\theta^3+6\theta-4=0. \tag{5}$$

It is easy to see that $\varepsilon=\theta^2+\theta-1$ is a unit in $R(\theta)$ and since this is just the ε defined by (2), it must be the fundamental unit of

$R(\theta)$. It is also easy to determine this unit from the relation $\theta = \dfrac{2}{\varrho + 1}$, i.e. $\varrho = \dfrac{2}{\theta} - 1$, which gives $\varepsilon = \varrho^2 + \varrho - 7 = \theta^2 + \theta - 1$.

As an example we here choose the relation (I, 16) of theorem 8 instead of (I, 15). Then $\varepsilon = \theta^2 + \theta - 1$ implies the substitution

$$\varphi = 2\theta + 1$$

and this gives

$$(\varphi^2 - 5)^n = U + V\varphi \tag{6}$$

where

$$\varphi^3 = 3\varphi^2 - 27\varphi + 57. \tag{7}$$

Hence by the notions of (I, 18) if $n \geq 0$ (6) may be written

$$\sum_{i=1}^{n} (-1)^i \binom{n}{i} \cdot 5^{n-i} \cdot a_{2i} = 0. \tag{6'}$$

Put $n = 3^p \cdot n_1$, $n_1 \not\equiv 0 \pmod 3$, $i = 3^q + r$. Then, if $0 \leq r < 3^q$, we have by lemma 9 and (7)

$$\binom{n}{i} \cdot a_{2i} \equiv 0 \left(\bmod 3^{p + \left[\frac{2i}{3}\right] - q}\right).$$

Now is

$$q \leq {}^3\log i < \left[\frac{2i}{3}\right], \text{ i.e. } \binom{n}{i} \cdot a_{2i} \equiv 0 \pmod{3^{p+1}}, \text{ if } i > 1.$$

Hence we get

$$\sum_{i=1}^{n} (-1)^i \cdot \binom{n}{i} \cdot 5^{n-i} \cdot a_{2i} \equiv \pm 3^p \pmod{3^{p+1}}$$

and (6') must be false, if $n \neq 0$. By lemma 7 n cannot be negative. $n = 0$ corresponds to $x = -2$.

(4) corresponds to the ring $R(\theta_1)$, defined by

$$\theta_1^3 - 6\theta_1^2 - 27\theta_1 - 24 = 0. \tag{8}$$

From the substitutions which gave (3) and (4) resp., we easily get the connection

$$\theta = \frac{2\theta_1 + 2}{3\theta_1 + 5}$$

and this gives

$$\varepsilon = \theta^2 + \theta - 1 = -\frac{\theta_1^2}{2} + \frac{9\theta_1}{2} + 1.$$

However

$$\varepsilon^2 = 8\,\theta_1^2 - 66\,\theta_1 - 71$$

belongs to $R(\theta_1)$ and hence is the fundamental unit of this ring. By theorem 8 we now write

$$6\,\theta_1 - \varepsilon^2 + 16\,\varepsilon + 55$$

and hence substitute

$$\varphi = \varepsilon + 8.$$

Then we can replace the equation $(\varepsilon^2)^n = u_1 + v_1\,\theta_1$ by

$$(\varphi - 8)^{2n} = U + V\,\varphi^2 \tag{9}$$

where

$$\varphi^3 - 9\,\varphi^2 + 9\,\varphi - 9 = 0.$$

Then by lemma 7 $n \geq 0$ and (9) may be written

$$\sum_{i=1}^{2n} (-1)^i \cdot \binom{2n}{i} \cdot 8^{2n-i} \cdot b_i = 0. \tag{9'}$$

Put as before $n = 3^p \cdot n_1$, $n_1 \not\equiv 0 \pmod 3$ and $i = 3^q + r$, $0 \leq r < 3^q$. Further we have the function congruence

$$\varphi^i \equiv 0 \left(\mathrm{mod}\ 3^{2\cdot\left[\frac{i}{3}\right]}\right)$$

and since

$$2 \cdot \left[\frac{i}{3}\right] - {}^3\log\, i \geq 1$$

if $i \geq 3$, we get as before $\binom{2n}{i} \cdot b_i \equiv 0 \pmod{3^{p+1}}$, if $i > 1$, and hence

$$\sum_{i=1}^{2n} (-1)^i \binom{2n}{i} \cdot 8^{2n-i} \cdot b_i \equiv \pm 3^p \pmod{3^{p+1}}$$

and (9') is not satisfied, if $n \neq 0$. $n = 0$ corresponds to $x = 13$. Hence the Diophantine equati on

$$y^2 - 12 \quad x^3$$

has exactly two integer solutions, namely

$$x = -2, \quad y = \pm 2 \quad \text{and}$$
$$x = 13, \quad y = \pm 47.$$

$f = 4$, i.e. *the equation* $y^2 - 48 = x^3$. By theorem 4 we only have to examine

$$\pm y + 4\sqrt{3} = (2 + \sqrt{3}) \cdot (a + b\sqrt{3})^3.$$

This gives

$$a^3 + 6a^2 b + 9ab^2 + 6b^3 = 4.$$

b must be odd, and since the congruence $a^3 + 6a^2 + 9a + 6 \equiv 0 \pmod 4$ has the single solution $a \equiv 2 \pmod 4$, we get only one form $G = 1$. The substitution $a = -2u + 3v$, $b = u + v$ gives

$$u^3 - 3uv^2 + 14v^3 = 1 \tag{10}$$

corresponding to the ring $R(\theta)$, defined by

$$\theta^3 - 3\theta - 14 = 0. \tag{11}$$

$R(\theta)$ belongs to $R(\varrho)$, defined by (1). We get

$$\theta = \frac{\varrho + 4}{\varrho}$$

i.e. $\varrho = \dfrac{4}{\theta - 1} = \dfrac{\theta^2 + \theta - 2}{4}$, which gives $\varepsilon = \varrho^2 + \varrho - 7 = \dfrac{1}{4}(\theta^2 + 5\theta - 22)$, where ε is the fundamental unit of $R(\varrho)$. Then

$$\varepsilon^2 = -\theta^2 - 11\theta + 39$$

is the fundamental unit of $R(\theta)$. By theorem 8 and $-6\theta = \varepsilon^2 + 4\varepsilon - 17$ we make the substitution

$$\varphi = \varepsilon + 2$$

which gives

$$(\varphi - 2)^{2n} = U + V\varphi^2 \tag{12}$$

where by lemma 7 $n \geq 0$ and where

$$\varphi^3 - 9\varphi^2 + 9\varphi - 63 = 0.$$

This gives

$$\sum_{i=1}^{2n} (-1)^i \cdot 2^{2n-i} \cdot \binom{2n}{i} \cdot b_i = 0. \tag{12'}$$

Put $n = 3^p \cdot n_1$, $n_1 \not\equiv 0 \pmod 3$ and $i = 3^q + r$, $0 \leq r < 3^q$. As in the determination of (9') we have $\varphi^i \equiv 0 \left(\mathrm{mod}\ 3^{2\cdot\left[\frac{i}{3}\right]}\right)$ and exactly in the same way we get

$$\sum_{i=1}^{2n} (-1)^i 2^{2n-i} \binom{2n}{i} b_i \equiv \pm 3^p \pmod{3^{p+1}}$$

if $n \neq 0$. $n = 0$ corresponds to $x = 1$. Hence the Diophantine equation

$$y^2 - 48 = x^3$$

has the only integer solution

$$x=1, \quad y=\pm 7.$$

$f=6$, i.e. *the equation* $y^2-108=x^3$. By theorem 4 we get all the solutions from

$$\pm y+6\sqrt{3}=\eta(a+b\sqrt{3})^3$$

$\eta=1$ gives

$$3a^2b+3b^3=6$$

with the solution $a=1$, $b=1$, corresponding to $x=-2$, $y=\pm 10$. $\eta=2+\sqrt{3}$ gives

$$a^3+6a^2b+9ab^2+6b^3=6$$

which by theorem 6 can give at most 2 forms $G=1$. These forms correspond to $a\equiv 0$ and 3 (mod 6). The substitution $a=-3u+6v$, $b=u$ gives

$$u^3-18uv^2+36v^3=1 \tag{13}$$

and the substitution $a=-6v_1$, $b=u_1+3v_1$ gives

$$u_1^3+9u_1v_1^2+18v_1^3=1. \tag{14}$$

(13) corresponds to the ring $R(\theta)$, defined by

$$\theta^3=18\theta+36 \tag{15}$$

and with the fundamental unit $\varepsilon=\theta-5$, which is just ε defined by (2). Then we have the condition

$$(\theta-5)^n=u+v\theta \tag{16}$$

where, by lemma 6, $n\geq 0$. This gives

$$\sum_{i=2}^{n}(-1)^i\cdot 5^{n-i}\cdot\binom{n}{i}\cdot a_i=0. \tag{16'}$$

As before we put $n=3^p\cdot n_1$, $n_1\not\equiv 0$ (mod 3) and $i=3^q+r$, $0\leq r<3^q$. By (15) we have $\theta^i\equiv 0 \pmod{3^{2\cdot\left[\frac{i}{3}\right]}}$ and hence we get exactly as for (9′) and (12′)

$$\sum_{i=2}^{n}(-1)^i\cdot 5^{n-i}\cdot\binom{n}{i}\cdot a_i\equiv\pm 3^p \pmod{3^{p+1}}$$

if $n>1$. $n=0$ corresponds to $x=6$, $y=\pm 18$ and $n=1$ corresponds to $x=366$, $y=\pm 7002$.

(14) corresponds to the ring $R(\theta_1)$, defined by

$$\theta_1^3+9\theta_1-18=0. \tag{17}$$

We get

$$\varrho=\frac{3\varrho}{\varrho+2}$$

i.e.

$$\varrho=\frac{2\theta_1}{3-\theta_1}=\frac{\theta_1^2}{6}+\frac{\theta_1}{2}-1.$$

Then $\varepsilon=\varrho^2+\varrho-7=\frac{\theta_1^2}{2}+\frac{\theta_1}{2}-2$, where ε, defined by (2), is the fundamental unit of $R(\varrho)$. Then

$$\varepsilon^2=-4\theta_1^2-2\theta_1+13$$

is the fundamental unit of $R(\theta_1)$. Now $2\theta_1=\varepsilon^2+8\varepsilon+3$. In this case the use of theorem 8 will be more laborious because $1\not\equiv 8 \pmod 3$. Put

$$\varphi=\varepsilon+4.$$

Then we get

$$(\varphi-4)^{2n}=U+V\varphi^2 \tag{18}$$

where

$$\varphi^3-3\varphi^2+15\varphi-53=0.$$

From the origin condition

$$\varepsilon^{2n}=u_1+v_1\theta_1$$

we see that $n<0$ is impossible since, if $v_1\neq 0$

$$u_1+v_1\theta_1=\frac{1}{(u_1+v_1\theta_1')(u_1+v_1\theta_1'')}=\frac{1}{u_1^2-u_1v_1\theta_1+\frac{18v_1^2}{\theta_1}}$$

where $1<\theta_1<2$. Hence $0<u_1+v_1\theta_1<1$ and $n>0$.

As always before we write $\varphi^i=a_i\varphi^2+b_i\varphi+c_i$, where a_i, b_i and c_i satisfy the recursion formula

$$x_i=-3x_{i-1}+15x_{i-2}+53x_{i-3}.$$

Then, if $i=2^r\cdot q$, q odd and $r\geq 2$, it is easy to show by induction that

$$a_i\equiv -q\cdot 2^{r+1},\ b_i\equiv q\cdot 2^{r+1} \text{ and } c_i\equiv 1 \pmod{2^{r+3}}. \tag{19}$$

Then we can calculate a convenient congruence for b_{i+k}, where $0<k<2^r$, by

$$b_{i+k} = a_i b_{k+2} + b_i b_{k+1} + c_i b_k.$$

Since $b_i \equiv i \pmod 4$ if i is odd and $\equiv 0 \pmod 4$ if i is even, this gives the formula

$$b_{2^r \cdot q+k} \equiv (-1)^{\left[\frac{k+q-1}{2}\right]} \cdot 2^{r+1} + b_k \pmod{2^{r+3}}. \tag{20}$$

As in (I, 15″) we now write

$$\sum_{i=0}^{2n} (-1)^i \cdot 4^i \binom{2n}{i} \cdot b_{2n-i} = 0. \tag{18′}$$

By (19) $2n = 2^p \cdot q$, $p \geq 2$, q odd implies

$$\sum_{i=0}^{2n} (-1)^i \cdot 2^{2i} \cdot \binom{2n}{i} \cdot b_{2n-1} \equiv 2^{p+1} \pmod{2^{p+2}}.$$

Then $2n \equiv 2 \pmod 4$, but this implies

$$b_{2n} \equiv 8 \pmod{16}$$

which gives $2n \equiv 6 \pmod 8$, as we see from the recursion formula. Put $2n = 2^p \cdot q + 6$, $p \geq 3$. (18′) and (20) give

$$(-1)^{\left[\frac{k+q-1}{2}\right]} \cdot 2^{p+1} + b_k - 2^{p+2} - 4kb_{k-1} + \sum_{i=2}^{2n} (-1)^i \cdot 2^{2i} \cdot \binom{2n}{i} \cdot b_{2n-i} \equiv$$

$$\equiv 0 \pmod{2^{p+3}}$$

and since $k = 6$ we get

$$(-1)^{\frac{q+1}{2}} \cdot 2^{p+1} + 312 - 2^{p+2} - 24 \cdot 201 \equiv 2^7 \pmod{2^8}.$$

This implies at first $p = 4$ and then $q \equiv 1 \pmod 4$, but this doesn't satisfy the congruence. Then (18) has no solution with $n \neq 0$. $n = 0$ corresponds to $x = -3$, $y = \pm 9$. We can get the same result in a little easier way, since the necessary condition $(2\varepsilon)^{2n} = (\theta_1^2 + \theta_1 - 4)^{2n} = U + V\theta_1$ implies that n is divisible by 9 but not by 3^3, while the same condition written $(\varepsilon^2)^n = (-4\theta_1^2 - 2\theta_1 + 13)^n = U + V\theta_1$ implies that $n \equiv 0 \pmod{3^3}$. Hence the Diophantine equation

$$y^2 - 108 = x^3$$

has exactly the four integer solutions

$$x = -3, \qquad y = \pm 9$$
$$x = -2, \qquad y = \pm 10$$
$$x = 6, \qquad y = \pm 18 \quad \text{and}$$
$$x = 366, \qquad y = \pm 7002.$$

The first case that can give forms corresponding to rings, which do not belong to $R(\varrho)$, is $f = 11$, i.e. the equation $y^2 - 363 = x^3$.

4. The equations $y^2 - 5f^2 = x^3$

As remarked by theorem 4, there can be solutions only of the reducible form $3a^2b + 5b^3 = 8f$, if f satisfies the cenditions of this theorem and is not divisible by 4. Hence $f = 1$ gives the only solution $(-1, \pm 2)$ and $f = 5$ the only solution $(-5, 0)$. $f = 2$ and 3 give insoluble equations. I shall here treat the case $f = 4$.

$f = 4$, i.e. *the equation* $y^2 - 80 = x^3$. By theorem 4 we have to examine

$$3a^2b + 5b^3 = 32$$

with the only solution $a = 3$, $b = 1$, corresponding to $x = 1$, and

$$\pm y + 4\sqrt{5} = \frac{1 + \sqrt{5}}{2} \cdot (a + b\sqrt{5})^3$$

which gives

$$a^3 + 3a^2b + 15ab^2 + 5b^3 = 8. \tag{1}$$

The substitution $a = 2u + v$, $b = -v$ gives

$$u^3 + 3uv^2 + v^3 = 1 \tag{2}$$

and since $a \equiv b \pmod 2$, (2) must contain all the solutions of (1).

(2) corresponds to the ring $R(\varepsilon)$, defined by

$$\varepsilon^3 + 3\varepsilon - 1 = 0. \tag{3}$$

$R(\varepsilon)$ is a fundamental ring and $D(\varepsilon) = -135$. (2) has the three solutions $(1, 0)$, $(0, 1)$ and $(1, -3)$, which correspond to $x = -4$, 4 and 44 resp.

Then the Diophantine equation

$$y^2 - 80 = x^3$$

has exactly the four integer solutions

$$x=-4, \quad y=\pm 4$$
$$x=1, \quad y=\pm 9$$
$$x=4, \quad y=\pm 12 \quad \text{and}$$
$$x=44, \quad y=\pm 292.$$

If $k=5$ and f (not necessarily cube-free) satisfies the conditions of theorem 4, x odd cannot correspond to an irreducible form. Then, since x even implies f exactly divisible by 2^m, where $m \equiv 2 \pmod 3$, all the irreducible forms must correspond to rings belonging to $R(\varepsilon)$. The first case, which can give forms not belonging to that ring, is $f=11$, i.e. the equation $y^2-605=x^3$.

5. The equations $y^2-6f^2=x^3$

$f=1$ gives an insoluble equation as both Mordell and Delaunay has shown. We get the insoluble form $(2, 0, 3, 2)=1$, which corresponds to the ring $R(1, \alpha, \beta)$, defined by

$$\begin{aligned} &\alpha^3+6\alpha-8=0 \\ &\beta^3-3\beta^2-8=0 \quad \text{and} \\ &\alpha\beta=4. \end{aligned} \tag{1}$$

$R(1, \alpha, \beta)$ is a fundamental ring and it has the fundamental unit $\varepsilon=\alpha-1$. $f=4$ gives an insoluble equation. I shall here treat the cases $f=2$ and 3.

$f=2$, i.e. *the equation* $y^2-24=x^3$. By theorem 4 we get

$$\pm y+2\sqrt{6}=(5+2\sqrt{6})\cdot(a+b\sqrt{6})^3$$

which gives

$$2a^3+15a^2b+36ab^2+30b^3=2.$$

The substitution $a=-2u+2v$, $b=u$ gives

$$u^3+6uv^2+8v^3=1 \tag{2}$$

and the substitution $a=u_1-5v_1$, $b=2v_1$ gives

$$u_1^3-3u_1v_1^2+10v_1^3=1. \tag{3}$$

(2) corresponds to the ring $R(\alpha)$, defined by the first equation (1). The fundamental unit is $\varepsilon=\alpha-1$. Then we have the condition

$$(\alpha-1)^n=u+v\alpha \tag{4}$$

which, except the cases $n=0$ and 1 can have one solution more with $n>1$. (4) can be replaced by

$$(4') \qquad \sum_{i=2}^{n}(-1)^i\cdot\binom{n}{i}\cdot a_i=0.$$

This equation is satisfied by $n=4$ and $(\alpha-1)^4=28\alpha-31$ gives the third solution $(-31, 28)$ of (2). $(1, 0)$ corresponds to $x=-2$, $y=\pm 4$, $(-1, 1)$ to $x=10$, $y=\pm 32$ and $(-31, 28)$ to $x=8158$, $y=\pm 736844$.

(3) corresponds to the ring $R(\theta)$, defined by

$$(5) \qquad \theta^3=3\theta+10.$$

$R(\theta)$ is identical with the ring $R(\beta)$, defined by the second equation (1). $\beta=\theta+1$. Either by (1) or by the transformations which gave (2) and (3) we then easily determine that $\varepsilon=\frac{\theta^2}{2}-\frac{\theta}{2}-2$. Then

$$\varepsilon^2=-\theta^2-3\theta-1$$

is the fundamental unit of $R(\theta)$. Since $\theta=\frac{\alpha^2}{2}+2$, we get by theorem 8 ($n\geq 0$ by lemma 7)

$$(6) \qquad (\alpha-1)^{2n}=U+V\alpha^2.$$

The impossibility of (6) for $n\neq 0$ follows exactly as for (8) in the case $y^2-8=x^3$. Lemma 10 is applicable and we get the same recursion formula as (9) in the said case. $n=0$ corresponds to $x=1$, $y=\pm 5$. Then the Diophantine equation

$$y^2-24=x^3$$

has exactly the four integer solutions

$$\begin{aligned} x&=-2, & y&=\pm\ 4\\ x&=\ 1, & y&=\pm\ 5\\ x&=10, & y&=\pm 32\\ x&=8158, & y&=\pm 736844. \end{aligned}$$

$f=3$, i.e. *the equation* $y^2-54=x^3$. Then we only have

$$\pm y+3\sqrt{6}=(5+2\sqrt{6})\cdot(a+b\sqrt{6})^3$$

which gives

$$2a^3+15a^2b+36ab^2+30b^3=3.$$

The substitution $a=-3u+3v$, $b=u$ gives

(7) $$u^3 - 9uv^2 + 18v^3 = 1$$

which by theorem 6 must contain all the solutions of the equation. (7) corresponds to the ring $R(\gamma)$, defined by

(8) $$\gamma^3 = 9\gamma + 18.$$

Here we have the relation

$$\gamma = \frac{6}{\theta - 1} = \frac{\theta^2}{2} + \frac{\theta}{2} - 1$$

where θ is defined by (5). Then we easily show that

$$\varepsilon^3 = -\gamma^2 - 3\gamma + 25$$

is the fundamental unit of $R(\gamma)$, where ε, defined by

$$\varepsilon^3 + 3\varepsilon^2 + 9\varepsilon - 1 = 0$$

is the fundamental unit of the fundamental ring $R(1, \alpha, \beta)$, defined by (1). Then $2\gamma = \varepsilon^2 + 4\varepsilon + 7$, by theorem 8 proposes the substitution

$$\varphi = \varepsilon + 2$$

and we get the condition

(9) $$(\varphi - 2)^{3^n} = U + V\varphi^2$$

where $n \geq 0$ by lemma 7 and

$$\varphi^3 = 3\varphi^2 - 9\varphi + 15.$$

(9) may be written

(9′) $$\sum_{i=1}^{3^n} (-2)^{3^n - i} \cdot \binom{3^n}{i} \cdot b_i = 0$$

and as before we put $3n = 3^p \cdot n_1$ and $i = 3^q + r$. Then, since $b_3 = -3^2$, we get by lemma 9

$$\sum_{i=1}^{3^n} (-2)^{3^n - i} \cdot \binom{3^n}{i} \cdot b_i \equiv \pm 3^p \pmod{3^{p+1}}$$

and hence there is no solution with $n \neq 0$. $n = 0$ corresponds to $x = 3$. The solution of $y^2 - 54 = x^3$ is equivalent to the solution of

(10) $$3Y^2 - 2 = X^3$$

and hence we have proved that (10) has the only solution $X = 1$, $Y = \pm 1$. (10) is solved by Nagell [7]. The Diophantine equation

$$y^2-54=x^3$$

has the only integer solution $x=3$, $y=\pm 9$.

$f=5$, i.e. the equation $y^2-150=x^3$, is the first case, where we by theorem 5 get forms not belonging to $R(1, \alpha, \beta)$.

6. The equations $y^2-7f^2=x^3$

The case $f=1$, i.e. the equation $y^2-7=x^3$, has been shown insoluble by V. A. Lebesgue. By theorem 4 this equation gives the irreducible form $(2, 0, -3, 3)=1$, corresponding to the ring $R(1, \alpha, \beta)$, where

$$\alpha^3-6\alpha-12=0 \tag{1}$$

$$\beta^3+3\beta^2-18=0 \quad \text{and} \tag{2}$$

$$\alpha\beta=6.$$

A unit in $R(\alpha)$ is $\varepsilon=-3\alpha^2+11\alpha-5$ and we shall show that ε is the fundamental unit in the fundamental ring $R(1, \alpha, \beta)$. Since $\beta=\frac{6}{\alpha}=\frac{\alpha^2}{2}-3$, we can write $R(1, \alpha, \beta)=R\left(1, \alpha, \frac{\alpha^2}{2}\right)$. Now suppose

$$\varepsilon=\eta^m=\left(\frac{x}{2}\cdot\alpha^2+y\alpha+z\right)^m=-3\alpha^2+11\alpha-5$$

where x, y, z and m are rational integers, $m\geq 2$. We get

$$x=\pm\frac{1}{\sqrt{756}}[(\alpha''-\alpha')\eta+(\alpha-\alpha'')\eta'+(\alpha'-\alpha)\eta''].$$

Since

$$\varepsilon^3+51\varepsilon^2+1221\varepsilon-1=0 \tag{3}$$

we get $|\varepsilon'|<35$, $3<\alpha<3\frac{1}{2}$ and $|\alpha'|<2$. This implies $x=0$, if $m>4$, $|x|\leq 1$, if $m=3$, and $|x|\leq 2$, if $m=2$. Now $x=0$ implies

$$|D(\varepsilon)|\geq y^6\cdot|D(\alpha)|$$

i.e. $|y|<11$, which is not satisfied. The remaining cases for $m=2$ and 3 can easily be shown impossible. Hence

$$\varepsilon=-3\alpha^2+11\alpha-5=11\alpha-6\beta-23$$

is the fundamental unit of $R(1, \alpha, \beta)$. I shall here treat $f=2$ and partly $f=3$, which is the first case, where forms belonging to other fields appear.

$f=2$, i.e. *the equation* $y^2-28=x^3$. We have

$$\pm y+2\sqrt{7}=(8+3\sqrt{7})\cdot(a+b\sqrt{7})^3$$

which by the substitution $a=-3b+c$ gives

$$2b^3-3bc^2+3c^3=2.$$

$b=u$, $c=2v$ gives

$$u^3-6uv^2+12v^3=1 \tag{4}$$

and $b=u_1-v_1$, $c=u_1+v_1$ gives

$$u_1^3+9u_1v_1^2+2v_1^3=1. \tag{5}$$

(4) corresponds to the ring $R(\alpha)$, defined by (1), with the fundamental unit $\varepsilon=-3\alpha^2+11\alpha-5$, defined by (3).

(5) corresponds to the ring $R(\theta)$, defined by

$$\theta^3+9\theta-2=0. \tag{6}$$

We find $\alpha=\dfrac{2+2\theta}{1-\theta}=\dfrac{\theta^2+\theta+6}{2}$ and hence $\varepsilon=\dfrac{5\theta^2+17\theta-4}{2}$. Then

$$\varepsilon^2=6\theta^2-404\theta+89$$

is the fundamental unit of $R(\theta)$.

To examine, whether (4) has a second solution, we determine $k\alpha=3\varepsilon^2+205\varepsilon+C$ and put

$$\varphi=6\varepsilon+205$$

which gives

$$(\varphi-205)^n=U+V\varphi^2. \tag{7}$$

This is a very unfavourable case for theorem 8. By (I, 15″) we write

$$\sum_{i=0}^{\infty}(-205)^i\cdot\binom{n}{i}\cdot b_{n-i}=0 \tag{7′}$$

which at first implies $b_n\equiv 0 \pmod 5$. Now

$$b_{k+24}\equiv b_k \pmod 5 \tag{8}$$

and the calculation of 24 consecutive values of b_k gives the necessary condition

$$n\equiv 0, 2, 15, 16 \text{ or } 19 \pmod{24}. \tag{9}$$

The recursion formula $b_k = a_3 b_{k-1} + b_3 b_{k-2} + c_3 b_{k-3}$ is still valid for $k<0$, but then b_k is not a rational integer. However, b_k is a 5-adic integer, which satisfies (8), and we get the same necessary condition (9), if $n<0$. Now we write

$$\varepsilon^n = (-3\alpha^2 + 11\alpha - 5)^n = u + v\alpha. \tag{10}$$

Since $\alpha^3 = 6(\alpha+2)$, we can consider powers of 2 and 3. Otherwise we could have substituted $\alpha = A\gamma + B$ to get a γ such that the p-adic function congruence $\gamma^3 \equiv 0 \pmod{p}$ were satisfied for any p. If we then write

$$(3\alpha^2 - 11\alpha)^i = A_i \alpha^2 + B_i \alpha + C_i$$

we get the condition (since $n \geq 0$ by lemma 7)

$$\sum_{i=1}^{n} 5^{n-i} \cdot \binom{n}{i} \cdot A_i = \sum_{i=1}^{n} t_i = 0 \tag{10'}$$

and, if $n \neq 0$, this immediately gives $n \equiv 1 \pmod 3$, i.e. by (9) $n \equiv 0$ or $3 \pmod 8$. $n = 2^p \cdot n_1$, n_1 odd and $p \geq 3$ implies

$$t_2 + t_4 \equiv 0 \pmod{2^{p+1}}$$

and $n \equiv 3 \pmod 8$ implies

$$t_1 + t_2 + t_3 \equiv 4 \pmod 8$$

but none of these congruences is satisfied. Then $n=0$ gives the only solution of (4) corresponding to $x=2$, $y = \pm 6$.

To examine, whether (5) has a second solution, we go on in the same manner. Since $k\theta = 5\varepsilon^2 - 12\varepsilon + C$ we put

$$\varphi = 5\varepsilon - 6$$

which gives

$$(\varphi + 6)^{2n} = U + V\varphi^2. \tag{11}$$

By (I, 15'') and since $n \geq 0$ by lemma 7 we write

$$\sum_{i=0}^{2n} 6^i \cdot \binom{2n}{i} \cdot b_{2n-i} = 0. \tag{11'}$$

In this case we get

$$b_{2k} \equiv 0, \quad b_{4k+1} \equiv 1 \text{ and } b_{4k-1} \equiv 3 \pmod 8$$

which also is true if $k<0$, since b_k is a 2-adic integer. Then we must have

$$2n \equiv 0 \pmod 4.$$

By induction we can prove the recursion formula

$$\varphi^{2^r} = 2^r \cdot a\,\varphi^2 + 2^{r+1} \cdot b\,\varphi + c \tag{12}$$

where a, b, c and r are rational integers, $a \equiv b \equiv c \equiv 1 \pmod 4$ and $r \geq 2$. By the relation $\varphi^{-k} \cdot \varphi^k = 1$ we get

$$\varphi^{-2^r} = -2^r \cdot a'\,\varphi^2 - 2^{r+1} \cdot b'\,\varphi + c' \tag{12'}$$

where $r \geq 2$ and a', b' and c' are 2-adic integers $\equiv 1 \pmod 4$. Further we see that $\varphi^{2^r \pm 2^s}$ is of the form (12) and $\varphi^{-2^r \pm 2^s}$ is of the form (12′) if $2 \leq r < s$.

Now suppose $2n = 2^p \cdot n_1$, n_1 odd and $p \geq 2$. Then (11′) gives the necessary condition

$$b_{2n} + 12n \cdot b_{2n-1} \equiv 2^{p+3} \pmod{2^{p+4}}$$

but this gives a contradiction in both the cases $n_1 \equiv 1$ and $-1 \pmod 4$. Then $n = 0$ gives the only solution of (5) corresponding to $x = -3$, $y = \pm 1$. Hence the Diophantine equation

$$y^2 - 28 = x^3$$

has exactly the two integer solutions

$$\begin{aligned} x &= -3, \qquad y = \pm 1 \quad \text{and} \\ x &= 2, \qquad y = \pm 6. \end{aligned}$$

$f = 3$, i.e. *the equation* $y^2 - 63 = x^3$. By theorem 5 and since the reducible form is insoluble, we have to examine the four equations

$$\begin{aligned} \pm y + 3\sqrt{7} &= (8 + 3\sqrt{7})\,(a + b\sqrt{7})^3 \\ \pm y + 3\sqrt{7} &= 3\eta\,(2 + \sqrt{7})\,(a + b\sqrt{7})^3 \end{aligned} \tag{13}$$

with $\eta = 1$ and $8 \pm 3\sqrt{7}$.

In the first case the substitution $a = u - 9v$, $b = 3v$ gives

$$u^3 - 3u^2 v + 18 v^3 = 1 \tag{14}$$

and by theorem 6 we get no other forms. (14) corresponds to $R(\beta)$, defined by (2), and we get $\varepsilon = \dfrac{11\beta^2}{3} + 5\beta - 23$. Hence

$$\varepsilon^3 = 2289\beta^2 - 6717\beta + 4447$$

is the fundamental unit of $R(\beta)$. Since $k\beta = 11\varepsilon^2 - 398\varepsilon + C$, we put

$$\varphi = 11\,\varepsilon + 199$$

which gives

$$(\varphi - 199)^{3^n} = U + V\varphi^2 \tag{15}$$

where $n \geq 0$ and

$$\varphi^3 \equiv 9\varphi^2 - 12\varphi + 12 \pmod{27}.$$

We write

$$\sum_{i=1}^{3^n} (-199)^{3^n - i} \cdot \binom{3^n}{i} \cdot b_i = \sum_{i=1}^{3^n} t_i = 0 \tag{15'}$$

and put $3n = 3^p \cdot n_1$, $n_1 \not\equiv 0 \pmod 3$, $i = 3^q + r$, $0 \leq r < 3^q$. Since $b_9 \equiv 0 \pmod{3^4}$ we get $t_i \equiv 0 \pmod{3^{p+2}}$ if $i > 6$, and, if $n \neq 0$, we get the necessary condition

$$t_1 + t_3 + t_4 + t_6 \equiv 0 \pmod{3^{p+2}}$$

which is not satisfied. Hence $n = 0$ gives the only solution of (14) corresponding to $x = 1$, $y = \pm 8$.

The other equations (13) give forms corresponding to other fields. $\eta = 1$ and $a = u + 2v$, $b = -v$ gives

$$u^3 + 9uv^2 + 12v^3 = 1 \tag{16}$$

which can have at most two solutions by lemma 2. We see that $v \equiv 0 \pmod 6$ and $u \equiv 1 \pmod{108}$. The solution $(1, 0)$ corresponds to $x = -3$, $y = \pm 6$.

$\eta = 8 - 3\sqrt{7}$ and $a = u + 2v$, $b = v$ gives

$$2u^3 - 3u^2v + 6uv^2 + 5v^3 = 1 \tag{17}$$

and $\eta = 8 + 3\sqrt{7}$ and $a = 3u - 2v$, $b = -u + v$ gives

$$2u^3 + 9uv^2 + 3v^3 = 1. \tag{18}$$

(16) corresponds to the fundamental ring $R(\theta)$ defined by

$$\theta^3 + 9\theta - 12 = 0. \tag{19}$$

In the field $K(\theta)$ we get the factorization $(2) = \mathfrak{p}^2 \cdot \mathfrak{p}_1$, $(3) = \mathfrak{q}^3$, $(\theta) = \mathfrak{p}_1^2 \cdot \mathfrak{q}$ and $(\theta - 1) = \mathfrak{p}$. This gives the unit

$$\varepsilon = \frac{(11\theta^2 - 5\theta - 9)^3}{3} = 36669\,\theta^2 - 163545\,\theta + 140365.$$

Suppose $\varepsilon = \eta^m$. We see easily modulo 2, 9 and 5 respectively that $m \neq 2$, 3 or 5. Then $m \geq 7$, $\varepsilon \sim \frac{1}{45} \cdot 10^{-10}$, $|\eta'| < 5.4$ and $|\theta - \theta'| < 3.7$

by Nagell's method imply that $\eta = u + v\theta$ with $|v| < 190800$ (or $|u| < 228900$). There is probably no such solution and then ε is the fundamental unit, but it is a deterrent limit for v or u though we know that $u \equiv 1 \pmod{108}$. If ε is fundamental then (16) has no second solution by lemma 8.

(17) is equivalent to $(2, 9, 18, 6) = 1$ and corresponds to the fundamental ring $R(1, \alpha, \beta)$, defined by

$$\begin{aligned} &\alpha^3 - 9\alpha^2 + 36\alpha - 24 = 0 \\ &\beta^3 - 18\beta^2 + 54\beta - 72 = 0 \\ &\alpha\beta = 12. \end{aligned} \tag{20}$$

In this field we have $(2) = \mathfrak{p}^2 \cdot \mathfrak{p}_1$, $(3) = \mathfrak{q}^3$, $(\alpha) = \mathfrak{p}^3 \cdot \mathfrak{q}$, $(\beta) = \mathfrak{p} \cdot \mathfrak{p}_1^2 \cdot \mathfrak{q}^2$ and $(1-\alpha) = \mathfrak{p}_1^2$. We get a unit $\varepsilon = \dfrac{(27\alpha^2 - 121\alpha + 81)^3}{3} \equiv 1 \pmod{3}$ and further $\lambda = \mathfrak{p} \cdot \mathfrak{q} \equiv \alpha - \beta \pmod{3}$ and $\mu = \mathfrak{p}_1 \equiv -\alpha - \beta - 1 \pmod{3}$.

(18) corresponds to the fundamental ring $R(1, \gamma, \delta)$, defined by

$$\begin{aligned} &\gamma^3 + 18\gamma - 12 = 0 \\ &\delta^3 - 9\delta^2 - 18 = 0 \\ &\gamma\delta = 6. \end{aligned} \tag{21}$$

Factorizations in this field give the unit $\varepsilon = -1602\gamma - 15792\delta + 146521$ which is neither square nor cube of a unit and further $\lambda = \mathfrak{p} = \delta - 8\gamma - 4$ and $\mu = \mathfrak{q} = 75 - 2\gamma - 6\delta$.

Then Delaunay's necessary conditions mentioned in chapter I are not satisfied if the calculated units are fundamental and on this presumption (17) and (18) are shown insoluble. I surrender working out this demonstration thoroughly. If nevertheless soluble they can of course have at most two solutions. Hence the Diophantine equation

$$y^2 - 63 = x^3$$

has the two solutions

$$\begin{aligned} x &= -3, \qquad y = \pm 6 \\ x &= 1, \qquad y = \pm 8 \end{aligned}$$

and there are in all probability no solutions more.

The first case which can give forms corresponding to other than these four fields is $f = 19$.

7. The equations $y^2 - 10f^2 = x^3$

$f = 1$, i.e. *the equation* $y^2 - 10 = x^3$. By theorem 4 we get

$$\pm y \mid 10 = (3 \mid 10) \cdot (a - b\sqrt{10})^3$$

which by the substitution $a = u + 3v$, $b = -v$ gives

$$u^3 + 3uv^2 + 6v^3 = 1. \tag{1}$$

The corresponding ring $R(\varrho)$ is defined by

$$\varrho^3 + 3\varrho - 6 = 0 \tag{2}$$

and we find easily as before the unit $\varepsilon = \frac{(-\varrho^2 - \varrho + 3)^3}{3} = -21\varrho^2 - 11\varrho + 49$, where

$$\varepsilon^3 - 273\varepsilon^2 + 19725\varepsilon - 1 = 0. \tag{3}$$

As before we also easily show that ε is the fundamental unit of the fundamental ring $R(\varrho)$. Since $k\varrho = 21\varepsilon^2 - 3260\varepsilon + C$ we put

$$\varphi = 21\varepsilon - 1630$$

and then we get

$$(\varphi + 1630)^n = U + V\varphi^2. \tag{4}$$

We have the formula

$$\varphi^{q \cdot 2^r} = 2^r \cdot a \cdot \varphi^2 + 2^r \cdot b \cdot \varphi + c$$

where q, a, b and c are odd integers and $r \geq 2$. If $q < 0$, a, b and c are duadic integers. This gives immediately $n \equiv 2 \pmod 4$. Lemma 7 gives $n \geq 0$. Now write the condition

$$[49 - \varrho \cdot (11 + 21\varrho)]^n = u + v\varrho. \tag{5}$$

Then if $\varrho^n \cdot (11 + 21\varrho)^n \doteq A_n\varrho^2 + B_n\varrho + C_n$ we must have $A_n \equiv 0 \pmod 7$, i.e. if $\varrho^n = a_n\varrho^2 + b_n\varrho + c_n$

$$a_n \equiv 0 \pmod 7.$$

Now $a_{k+48} \equiv a_k \pmod 7$ and we find $k \not\equiv 2 \pmod 4$ in all the cases where $a_k \equiv 0 \pmod 7$. Hence (1) has the only solution (1, 0) and the Diophantine equation

$$y^2 - 10 = x^3$$

has exactly one integer solution

$$x = -1, \quad y = \pm 3.$$

$f=2$, i.e. *the equation* $y^2-40=x^3$. Analogously to (1) we get

$$a^3+3ab^2+6b^3=2.$$

$a=2c$ gives

$$4c^3+3cb^2+3b^3=1 \tag{6}$$

and $a=-u+4v$, $b=u-2v$ gives

$$u^3-18uv^2+32v^3=1. \tag{7}$$

(6) corresponds to the ring $R(1,\alpha,\beta)$, defined by

$$\begin{aligned}&\alpha^3+12\alpha-48=0\\ &\beta^3-3\beta^2-36=0\\ &\alpha\beta=12.\end{aligned} \tag{8}$$

Since $\alpha=2\varrho$ and $\beta=\varrho^2+3$, where ϱ is defined by (2), we have $R(1,\alpha,\beta)=R(1,2\varrho,\varrho^2)$. In the field $K(\varrho)$ we get $(3)=\mathfrak{q}^3$ but $\mathfrak{q}=(-\varrho^2-\varrho+3)$ is no principle ideal of $R(1,2\varrho,\varrho^2)$ and hence (6) is insoluble by lemma 4.

(7) corresponds to the ring $R(\theta)$ defined by

$$\theta^3-18\theta-32=0. \tag{9}$$

We get $\varrho=\dfrac{\theta+4}{\theta+2}=\dfrac{\theta^2}{2}-\theta-6$, which gives the fundamental unit $\varepsilon=5\theta^2-31\theta+31$, where ε is defined by (3). In this case we keep the equation

$$\varepsilon^n=(5\theta^2-31\theta+31)^n=u+v\theta. \tag{10}$$

We write $\theta^i\cdot(5\theta-31)^i=A_i\theta^2+B_i\theta+C_i$ and find the recursion formulas with $k\geq 0$

$$\begin{aligned}
A_{1+8k}&\equiv -3\cdot 2^{4k} \pmod{2^{4k+3}} & A_{5+8k}&\equiv 2^{4k+2} \pmod{2^{4k+5}}\\
A_{2+8k}&\equiv 3\cdot 2^{4k} \pmod{2^{4k+3}} & A_{6+8k}&\equiv 3\cdot 2^{4k+2} \pmod{2^{4k+5}}\\
A_{3+8k}&\equiv 2^{4k+1} \pmod{2^{4k+4}} & A_{7+8k}&\equiv -3\cdot 2^{4k+3} \pmod{2^{4k+6}}\\
A_{4+8k}&\equiv 2^{4k+1} \pmod{2^{4k+4}} & A_{8+8k}&\equiv 2^{4k+3} \pmod{2^{4k+6}}.
\end{aligned}$$

Now we have

$$\sum_{i=1}^{\infty} 31^{n-i}\cdot\binom{n}{i}\cdot A_i=\sum_{i=1}^{\infty} t_i=0. \tag{10'}$$

From $t_1+t_2\equiv 0 \pmod 2$ we get $n\equiv 0$ or $-1 \pmod 4$.

A. $n \equiv 0 \pmod 4$. Suppose $n = 2^p \cdot n_1$, n_1 odd, $p \geq 2$. $p = 2$ is impossible modulo 2^4 and if $p > 2$ an examination modulo 2^{p+3} implies $p = 3$, which gives a contradiction modulo 2^{p+4}.

B. $n \equiv -1 \pmod 4$. In the same way we successively get the sharpened necessary condition $n \equiv 11 \pmod{32}$, but if we then make the substitution $\theta = \varphi - 2$ we have

$$\varepsilon^n = (5\varphi^2 - 51\varphi + 113)^n = U + V\varphi \tag{10''}$$

where

$$\varphi^3 = 6\varphi^2 - 6\varphi - 4.$$

This gives the corresponding formula $\sum_{i=1}^{\infty} 113^{n-i} \cdot \binom{n}{i} \cdot A_i' - \sum_{i=1}^{\infty} t_i' = 0$, but then the condition $t_1' + t_2' + t_3' + t_4' \equiv 8 \pmod{16}$ is not satisfied if $n \equiv 11 \pmod{32}$. Then (10) has only the solution $n = 0$ and the Diophantine equation

$$y^2 - 40 = x^3$$

has exactly one integer solution

$$x = 6, \quad y = \pm 16.$$

$f = 3$ gives an insoluble equation. The first case which can give forms corresponding to other fields is $f = 13$.

8. The equations $y^2 - 11f^2 = x^3$

It has been known a long time that the equation $y^2 - 11 = x^3$ has no integer solutions. The equation corresponds to the insoluble form

$$2u^3 + 3uv^2 + 3v^3 = 1 \tag{1}$$

which belongs to the fundamental ring $R(1, \alpha, \beta)$ defined by

$$\begin{aligned} &\alpha^3 + 6\alpha - 12 = 0 \\ &\beta^3 - 3\beta^2 - 18 = 0 \\ &\alpha\beta = 6. \end{aligned} \tag{2}$$

In this cubic field we get the factorizations $(2) = \mathfrak{p}^2 \cdot \mathfrak{p}_1$, $(2 - \alpha) = \mathfrak{p} \cdot \mathfrak{p}_1^2$ and $(\beta - 4) = \mathfrak{p}$ and this gives $4 \cdot \varepsilon = (2 - \alpha) \cdot (\beta - 4)^3$, i.e. $\varepsilon = -2\alpha + 24\beta - 95$ where

$$\varepsilon^3 + 213\varepsilon^2 + 9531\varepsilon - 1 = 0. \tag{3}$$

$R(1, \alpha, \beta) = R\left(1, \alpha, \frac{\alpha^2}{2}\right)$ or $R\left(1, \beta, \frac{\beta^2}{3}\right)$ and we can show as before that ε is the fundamental unit of the field.

$f = 2$, i.e. *the equation* $y^2 - 44 = x^3$. Since the reducible form is insoluble we only have

$$\pm y + 2\sqrt{11} = (10 + 3\sqrt{11}) \cdot (a + b\sqrt{11})^3$$

which by the substitution $a = d - 3c$, $b = c$ gives

$$2c^3 + 3cd^2 + 3d^3 = 2.$$

$c = u$, $d = 2v$ gives

$$u^3 + 6uv^2 + 12v^3 = 1 \tag{4}$$

and $c = u_1$, $d = -u_1 + 2v_1$ gives

$$u_1^3 + 3u_1^2 v_1 - 12u_1 v_1^2 + 12v_1^3 = 1. \tag{5}$$

(4) corresponds to the ring $R(\alpha)$, defined by (2), and we get the fundamental unit $\varepsilon = 12\alpha^2 - 2\alpha - 23$. Now since $n \geq 0$

$$(12\alpha^2 - 2\alpha - 23)^n = u + v\alpha$$

implies that $n \not\equiv -1 \pmod 3$ and modulo 9 that $n \not\equiv 1 \pmod 3$. Further $n \not\equiv 0 \pmod 3$ by lemma 8 if $n \neq 0$. Then (4) has the only solution (1, 0), corresponding to $x = -2$.

(5) corresponds to the ring $R(\gamma)$ defined by

$$\gamma^3 - 3\gamma^2 - 12\gamma - 12 = 0. \tag{6}$$

We have $\alpha = \frac{2\gamma}{2+\gamma} = \frac{1}{2} \cdot (-\gamma^2 + 5\gamma + 6)$ and $\varepsilon = 13\gamma^2 - 41\gamma - 173$ is the fundamental unit also in this ring.

$$(13\gamma^2 - 41\gamma - 173)^n = u_1 + v_1\gamma$$

implies that $n \not\equiv 1 \pmod 3$. Further $n \not\equiv 0 \pmod 3$ by lemma 8 if $n \neq 0$. We get successively the conditions $n \equiv 2 \pmod 9$ and $n \equiv -7 \pmod{27}$. Then we substitute $\gamma = \varphi + 3$, which gives

$$\varphi^3 + 6\varphi^2 - 3\varphi - 48 = 0 \tag{7}$$

and $\varepsilon = 13\varphi^2 + 37\varphi - 179$. The condition

$$(13\varphi^2 + 37\varphi - 179)^n = U + V\varphi$$

however, is not satisfied for $n \equiv -7 \pmod{27}$. Hence (5) has the

only solution (1, 0) corresponding to $x=5$, and the Diophantine equation

$$y^2-44=x^3$$

has exactly the two integer solutions

$$x=-2,\quad y=\pm 6$$
$$x=5,\quad y=\pm 13.$$

$f=3$, i.e. *the equation* $y^2-99=x^3$. The reducible form is insoluble and from

$$(y+3\sqrt{11})\,(10-3\sqrt{11})\cdot(a+b\sqrt{11})^3$$

comes by the substitution $a=u-9v$, $b=v$

$$u^3+3u^2v+18v^3=1 \tag{8}$$

which corresponds to the ring $R(\beta)$, defined by (2). We get $\varepsilon=-\frac{2\beta^2}{3}+26\beta-95$ and it is easily shown that ε^3 is the fundamental unit of $R(\beta)$. Since $k\beta=\varepsilon^2+1054\varepsilon+C$ we make the substitution $\varphi=\varepsilon+527$ and by theorem 8 we have

$$(\varphi-527)^{3^n}=U+V\varphi^2 \tag{9}$$

where $n\geq 0$ and $\varphi^3\equiv 3\varphi+3 \pmod 9$. (9) may as usual be written

$$\sum_{i=1}^{3^n}\binom{3^n}{i}\cdot(-527)^{3^n-i}\cdot b_i=0 \tag{9'}$$

but this is not satisfied modulo 3^{p+1}, if we suppose $3n=3^p\cdot n_1$, $n_1\not\equiv 0 \pmod 3$. Hence (8) has the only solution (1, 0) and the Diophantine equation

$$y^2-99=x^3$$

has exactly one integer solution

$$x=1,\quad y=\pm 10.$$

$f=5$ is the first case which can give forms corresponding to other fields.

9. The equations $y^2-13f^2=x^3$, $y^2-21f^2=x^3$ and $y^2-29f^2=x^3$

$k\equiv 5 \pmod 8$ and as pointed out after the proof of theorem 4, a necessary condition for a soluble irreducible form is that $f\equiv 2^{3t-1} \pmod{2^{3t}}$, if f satisfies the conditions of this theorem. The case

$f-4$ will give us the fundamental ring to which all these irreducible forms belong.

I. $k=13$. $f=1$ gives an insoluble equation.

$f=2$. i.e. *the equation* $y^2-52=x^3$. We have only to examine

$$3a^2b+13b^3=16$$

which has the solution $a=b=1$. Hence the Diophantine equation

$$y^2-52=x^3$$

has the only integer solution

$$x=-3, \quad y=\pm 5.$$

$f=4$, i.e. *the equation* $y^2-208=x^3$. The reducible form is insoluble and we only have

$$\pm y+4\sqrt{13}=\frac{3+\sqrt{13}}{2}\cdot(a+b\sqrt{13})^3$$

which by the substitution $a=2u-v$, $b=v$ gives

$$u^3+3u^2v+6uv^2+v^3=1. \tag{1}$$

Since $a\equiv b \pmod 2$ we get no more forms. (1) corresponds to $R(\varepsilon)$, where $D(\varepsilon)=-351$ and

$$\varepsilon^3=3\varepsilon^2-6\varepsilon+1. \tag{2}$$

Substituting $\varphi=\varepsilon-1$ in order to get $\varphi^3\equiv 0 \pmod 3$ we get the condition

$$(\varphi+1)^n=u+v+v\varphi \tag{3}$$

and we easily see that there are no solutions except $n=0$ and 1. Hence the Diophantine equation

$$y^2-208=x^3$$

has exactly the two integer solutions

$$x=-4, \qquad y=\pm 12$$
$$x=12, \qquad y=\pm 44.$$

Already in the case $f=3$, however, i.e. in the equation $y^2-117=x^3$, we have to examine forms belonging to another field $K(\theta)$, where $\theta^3=9\theta+24$.

II. $k = 21$. $f = 1$ and 2 give insoluble equations. If $f = 3$, the reducible form gives the only solution $x = -5$, $y = \pm 8$. $f = 4$, i.e. the equation $y^2 - 336 = x^3$, gives quite analogously to the case $k = 13$ the single form

$$u^3 - 3uv^2 + 5v^3 = 1. \tag{4}$$

The corresponding ring $R(\varrho)$, defined by $\varrho^3 - 3\varrho - 5 = 0$, is a fundamental ring with $D = -567$ and with the fundamental unit $\varepsilon = -\varrho^2 + \varrho + 3$, where

$$\varepsilon^3 = 3\varepsilon^2 - 12\varepsilon + 1. \tag{5}$$

By (I, 16) the substitution $\varphi = 2\varrho - 1$ gives

$$(\varphi^2 - 13)^n = U + V\varphi \tag{6}$$

with $\varphi^3 + 3\varphi^2 - 9\varphi - 51 = 0$. (6) implies immediately that $n \equiv 0 \pmod 3$ but this is impossible by lemma 8, if $n \neq 0$, and hence (4) has only the solution $(1, 0)$ and the equation $y^2 - 336 = x^3$ exactly one solution $x = 4$, $y = \pm 20$. $f = 5$ is the first case, where forms corresponding to other fields appear.

III. $k = 29$. $f = 1$, 2 and 3 give insoluble equations. $f = 4$, i.e. the equation $y^2 - 464 = x^3$, has the solution $x = -7$, $y = \pm 11$ from the reducible form and further we get as for $k = 13$ and 21

$$u^3 + 3uv^2 + 5v^3 = 1. \tag{7}$$

The corresponding ring $R(\theta)$ with $D = -783$ and defined by $\theta^3 + 3\theta - 5 = 0$ has the fundamental unit $\varepsilon^2 = \theta - 1$, where ε generates the fundamental ring $R(\varepsilon)$ with $D = -87$ and where

$$\varepsilon^3 + \varepsilon^2 + 2\varepsilon - 1 = 0. \tag{8}$$

The substitution $\varphi = \theta + 1$ gives

$$(\varphi - 2)^n = u - v + v\varphi \tag{9}$$

and $\varphi^3 = 3\varphi^2 - 6\varphi + 9$ and it is easy to show that (7) has only the solutions $(1, 0)$ and $(-1, 1)$. Hence $y^2 - 464 = x^3$ has exactly the three solutions $x = -7$, $y = \pm 11$; $x = -4$, $y = \pm 20$ and $x = 20$, $y = \pm 92$. The first case which gives forms corresponding to other fields is $f = 5$.

10. The equations $y^2 - 14f^2 = x^3$

The equation $y^2 - 14 = x^3$ is insoluble, which has been known a long time. We get the insoluble form

$$2u^3 - 3uv^2 + 4v^3 = 1 \tag{1}$$

corresponding to the fundamental ring $R(1, \alpha, \beta)$ defined by

$$\begin{aligned} &\alpha^3 - 6\alpha - 16 = 0 \\ &\beta^3 + 3\beta^2 - 32 = 0 \\ &\alpha\beta = 8. \end{aligned} \tag{2}$$

From the factorization $(2) = \mathfrak{p}^2 \cdot \mathfrak{p}_1$, $(3) = \mathfrak{q}^3$, $(\beta - 2) = \mathfrak{p}^2 \cdot \mathfrak{q}$ and $(\beta + 4) = \mathfrak{p}^4 \cdot \mathfrak{q}$ we get the unit $\varepsilon = \frac{1}{3} \cdot (3\alpha - 2\beta - 5)^3 = -63\alpha - 8\beta + 227 = -4\alpha^2 - 63\alpha + 251$, defined by

$$\varepsilon^3 - 705\varepsilon^2 + 201015\varepsilon - 1 = 0. \tag{3}$$

$R(1, \alpha, \beta) = R\left(1, \alpha, \frac{\alpha^2}{2}\right)$ and as before we show that ε is the fundamental unit of the field.

$f = 2$, i.e. *the equation* $y^2 - 56 = x^3$. The reducible form is insoluble and we get

$$\pm y + 2\sqrt{14} = (15 + 4\sqrt{14}) \cdot (a + b\sqrt{14})^3.$$

By theorem 6 we can get at most two forms. $a = -4u + 2v$, $b = u$ gives

$$u^3 - 6uv^2 + 16v^3 = 1 \tag{4}$$

and $a = u_1 - 7v_1$, $b = 2v_1$ gives

$$2u_1^3 + 3u_1^2 v_1 + 7v_1^3 = 1. \tag{5}$$

(4) corresponds to $R(\alpha)$, defined by (2). We substitute $\alpha = \varphi - 2$, which gives

$$\varphi^3 - 6\varphi^2 - 6\varphi - 12 = 0$$

and then we get the condition

$$\varepsilon^n = (-4\varphi^2 - 47\varphi + 361)^n = U + V\varphi.$$

This implies that $n \equiv 0 \pmod 3$, which is impossible by lemma 8, if $n \neq 0$. Then (4) has the only solution (1, 0) corresponding to $x = 2$.

Since we have $\gamma = \beta + 2$, where $\gamma^3 - 3\gamma^2 - 28 = 0$, we easily see that (5) corresponds to the ring $R(1, 2\alpha, \beta)$. By lemma 4 $\lambda = \mathfrak{p}_1$ but

$\mathfrak{p}_1=(-\alpha+\beta+1)$ doesn't belong to the ring and hence (5) is insoluble and the Diophantine equation

$$y^2-56=x^3$$

has exactly one integer solution

$$x=2,\quad y=\pm 8.$$

The first case which gives forms corresponding to other fields is $f=5$.

11. The equations $y^2-15f^2=x^3$

$f=1$, i.e. *the equation* $y^2-15=x^3$. As pointed out above this equation has exactly two solutions. The corresponding form is

$$u^3-3uv^2+8v^3=1 \tag{1}$$

with the solutions $(1, 0)$ and $(5, -2)$ and it is easy to show that $\varepsilon=5-2\varrho$, defined by

$$\varepsilon^3-15\varepsilon^2+63\varepsilon-1=0 \tag{2}$$

is the fundamental unit of the corresponding fundamental ring $R(\varrho)$. The Diophantine equation

$$y^2=15=x^3$$

has the two solutions

$$x=1,\quad y=\pm 4$$
$$x=109,\quad y=\pm 1138.$$

The case $f=6$ will be of current interest in chapter III. We get the form $u^3-3uv^2+8v^3=6$, which can be substituted by the two forms $(1, 0, 18, 36)=1$ and $(1, 0, -63, 198)=1$. The corresponding rings have both the fundamental unit ε^3. Theorem 8 proposes the substitutions $\varphi=\varepsilon-4$ and $\varphi=\varepsilon-7$ resp., and we easily see that each form has the only solution $(1, 0)$, i.e. the equation $y^2-540=x^3$ has the two solutions $x=-6$, $y=\pm 18$ and $x=21$, $y=\pm 99$.

The first case, which gives forms not belonging to $R(\varrho)$, is $f=7$.

12. The equations $y^2-17f^2=x^3$

Since $17\equiv 1 \pmod 8$, we must always consider the prime 2, which divides into two different primes in $K(\sqrt{17})$. Nagell has solved the case $f=1$ [7]. Except the insoluble reducible form there are by

theorem 5 four irreducible forms, which all are soluble and correspond to rings from different fields. Those rings are $R(\alpha)$ with the fundamental unit $\varepsilon_1 = 2\alpha - 3$ and defined by

$$\alpha^3 = -3\alpha + 8, \tag{1}$$

$R(\beta)$ with the fundamental unit $\varepsilon_2 = \beta - 3$, where

$$\beta^3 = 6\beta + 10, \tag{2}$$

$R(\gamma)$ with the fundamental unit $\varepsilon_3 = -3\gamma^2 + 6\gamma + 25$ and with

$$\gamma^3 = 12\gamma + 18 \tag{3}$$

and $R(\delta)$ with the fundamental unit $\varepsilon_4 = -\delta + 1$ and defined by

$$\delta^3 = -6\delta + 6. \tag{4}$$

$R(\alpha)$ belongs to the fundamental ring $R(\varrho)$ with $D(\varrho) = -459$ and defined by

$$\varrho^3 = 6\varrho + 7. \tag{5}$$

We have $\varrho = -\dfrac{\alpha - 3}{\alpha - 1}$ and hence $\varepsilon_1 = 2\alpha - 3 = 2\varrho^2 - 2\varrho - 11$. By Nagell's method we easily show that ε_1 is the fundamental unit of $R(\varrho)$. We have

$$\varepsilon_1^3 + 9\varepsilon_1^2 + 39\varepsilon_1 - 1 = 0. \tag{6}$$

$R(\beta)$ is a fundamental ring and ε_2 is defined by

$$\varepsilon_2^3 + 9\varepsilon_2^2 + 21\varepsilon_2 - 1 = 0. \tag{7}$$

$R(\gamma)$ belongs to the fundamental ring $R(\sigma)$, where $D(\sigma) = -204$ and

$$\sigma^3 = \sigma^2 - \sigma + 3. \tag{8}$$

$\varepsilon_3 = -\sigma^2 + \sigma + 1$ is the fundamental unit of $R(\sigma)$ and we have

$$\varepsilon_3^3 - 5\varepsilon_3^2 + 11\varepsilon_3 - 1 = 0. \tag{9}$$

$R(\delta)$ is a fundamental ring and ε_4 is defined by

$$\varepsilon_4^3 - 3\varepsilon_4^2 + 9\varepsilon_4 - 1 = 0. \tag{10}$$

Then every equation $y^2 - 17f^2 = x^3$, where f, except eventually 2 and 17, contains only primes of the second degree in $K(\sqrt{17})$, must have all of the irreducible forms corresponding to rings, which belong to any of those four fields. I shall here treat the case $f = 2$. $f = 13$ is the first case that can give forms belonging to other fields.

$f = 2$, i.e. *the equation* $y^2 - 68 = x^3$. By theorem 5 we have to examine

$$\pm y + 2\sqrt{17} = \eta (a + b\sqrt{17})^3$$

where $\eta = 1$ of course gives an insoluble form and $\eta = 4 + \sqrt{17}$ gives

$$a^3 + 12a^2 b + 51ab^2 + 68b^3 = 2$$

which is impossible modulo 9, and

$$\pm y + 2\sqrt{17} = \eta (5 + \sqrt{17}) \cdot \left(\frac{a + b\sqrt{17}}{2}\right)^3 .$$

$\eta = 1$ gives

$$a^3 + 15a^2 b + 51ab^2 + 85b^3 = 16$$

which is impossible modulo 9.

$\eta = 4 - \sqrt{17}$ gives

$$-a^3 + 9a^2 b - 51ab^2 + 51b^3 = 16$$

which is impossible modulo 9 too.

$\eta = 4 + \sqrt{17}$ gives

$$9a^3 + 111a^2 b + 459ab^2 + 629b^3 = 16.$$

We get the necessary condition a and b both odd and $a \equiv b \pmod 4$. Then we cannot loose any solution by the substitution

$$a = 5u - 6v, \quad b = -u + 2v$$

which gives

$$u^3 + 12uv^2 + 4v^3 = 1. \tag{11}$$

The corresponding ring $R(\theta)$, defined by

$$\theta^3 + 12\theta - 4 = 0 \tag{12}$$

belongs to $R(\gamma)$ and the fundamental unit is just $\varepsilon_3 = 25 + 6\gamma - 3\gamma^2 = 1 - 3\theta$, since $\gamma = \frac{\theta^2}{2} + 4$. Then (11) has the solutions (1, 0) and (1, −3) and by lemma 1 there cannot be a third solution, since $D(\varepsilon) \neq D(\theta)$. The two solutions correspond to $x = -4$ and 152 resp. and the Diophantine equation

$$y^2 - 68 = x^3$$

has exactly the two integer solutions

$$x = -4, \qquad y = \pm 2 \quad \text{and}$$
$$x = 152, \qquad y = \pm 1874.$$

13. The equations $y^2-19f^2=x^3$

$f=1$, i.e. *the equation* $y^2-19=x^3$. The reducible form is insoluble and

$$\pm y+\sqrt{19}=(170+39\sqrt{19})\cdot(a+b\sqrt{19})^3$$

gives by the substitution $a=-9u+22v$, $b=2u-5v$

$$u^3-15uv^2+24v^3=1 \tag{1}$$

corresponding to the fundamental ring $R(\varrho)$, defined by

$$\varrho^3-15\varrho-24=0. \tag{2}$$

In the field $K(\varrho)$ we get $(3)=\mathfrak{q}^3$ and $\mathfrak{q}=(2\varrho-9)$, which gives $\varepsilon=-\frac{(2\varrho-9)^3}{3}=-36\varrho^2+202\varrho-179$ with

$$\varepsilon^3+1617\varepsilon^2+685887\varepsilon-1=0. \tag{3}$$

Suppose $\varepsilon=(w\varrho^2+v\varrho+u)^m$. We see easily that $m\neq 2$, 3 or 5 and then Nagell's method gives $w=0$ and $|v|<176$, which is not satisfied. Hence ε is the fundamental unit of the field. The condition $\varepsilon^n=u+v\varrho$ may be treated modulo powers of 2 or 3. We choose 2 and put $\varphi=2\varrho$. Then $n\geq 0$ by lemma 7 and

$$(-9\varphi^2+101\varphi-179)^n=u+\frac{v}{2}\cdot\varphi \tag{4}$$

implies that $n\equiv 11 \pmod{64}$, but writing $\varphi=\psi-4$ we get

$$(-9\psi^2+173\psi-727)^n=u-2v+\frac{v}{2}\cdot\psi \tag{4'}$$

where $n\equiv 11 \pmod{32}$ implies that $n\equiv -21 \pmod{64}$. Then (1) has only the solution (1, 0) and the Diophantine equation

$$y^2-19=x^3$$

has exactly one integer solution

$$x=5,\quad y=\pm 12.$$

$f=2$, i.e. *the equation* $y^2-76=x^3$. The reducible form is insoluble and

$$\pm y+2\sqrt{19}=(170+39\sqrt{19})\cdot(a+b\sqrt{19})^3$$

gives by the substitution $a=4u-14v$, $b=-u+3v$

$$u^3+9uv^2+14v^3=1 \tag{5}$$

and by the substitution $a = -5u_1 - 18v_1$, $b = u_1 + 4v_1$

$$3u_1^3 + 12u_1^2 v_1 + 18u_1 v_1^2 + 4v_1^3 = 1. \tag{6}$$

(5) corresponds to the ring $R(\theta)$, defined by

$$\theta^3 + 9\theta - 14 = 0. \tag{7}$$

We get $\varepsilon = 65\theta^2 + 29\theta - 149$. Putting $\theta = \varphi - 1$ we have $n \geq 0$ and

$$(65\varphi^2 - 101\varphi - 113)^n = u - v + v\varphi$$

which implies that $n \equiv 0 \pmod 3$ but this is impossible by lemma 8, if $n \neq 0$. Hence (5) has only the solution $(1, 0)$ corresponding to $x = -3$.

(6) corresponds to the ring $R(1, \alpha, \beta)$, defined by

$$\begin{aligned} &\alpha^3 - 12\alpha^2 + 54\alpha - 36 = 0 \\ &\beta^3 - 18\beta^2 + 48\beta - 48 = 0 \\ &\alpha\beta = 12. \end{aligned} \tag{8}$$

It is easy to see that $R(1, \alpha, \beta) = R(1, 2\varrho, \varrho^2 + \varrho)$ and hence consists of all integers $A\varrho^2 + B\varrho + C$ with $A \equiv B \pmod 2$. We get $\varepsilon = -36\alpha + 47\beta - 677$, $\lambda = \mathfrak{q} = \beta - 15$ and $\mu = \mathfrak{p} \cdot \mathfrak{p}_1 = -5\alpha + 4$. Delaunay's conditions, mentioned in chapter I, are satisfied but not identically and his method proposes the first raised form $(3, 12, 18, 4) \cdot \begin{pmatrix} 235 & 111k \\ 36 & 17k \end{pmatrix}$ with $k = F(36, 47)$, $F(u, v) = (3, 12, 18, 4)$. Corresponding to λ and μ we get $\lambda_1 = -235\alpha + 180\beta + 3381$ and $\mu_1 = (111\alpha - 85\beta - 1597) \cdot k$ and a necessary condition is that $\lambda_1 \cdot \varepsilon^t$ and $\mu_1 \cdot \varepsilon^{t'}$ be integers of the raised ring for any t and t', $0 \leq t$, $t' < m$, ε^m fundamental unit of this new ring. Probably this is not the fact and then (6) would be shown insoluble but I surrender working out this demonstration. In any case (6) can have at most two solutions. Hence the Diophantine equation

$$y^2 = 76 \cdot x^3$$

has the integer solution

$$x = -3, \quad y = \pm 7$$

and probably no solutions more.

Already $f = 3$ gives forms corresponding to other fields.

The treatment of the following cases will be rendered more briefly.

14. The equations $y^2 - 31f^2 = x^3$

$f = 1$, i.e. *the equation* $y^2 - 31 = x^3$. As before we get the only form

(1) $$u^3 + 9uv^2 + 4v^3 = 1.$$

In the corresponding fundamental ring $R(\varrho)$, defined by $\varrho^3 + 9\varrho - 4 = 0$, we find the unit $\varepsilon = 821\varrho^2 + 109\varrho - 203$, where

(2) $$\varepsilon^3 + 15387\varepsilon^2 + 59753877\varepsilon - 1 = 0.$$

Nagell's method gives that ε is the fundamental unit if (1) has no solution with $|v| < 1158$ or hence $|u| < 0.45 \cdot |v| < 522$. We get $u \equiv 1 \pmod{36}$ and further $u \equiv \pm 2 \pmod 5$, $0 \pmod 7$, $-3 \pmod{16}$, $5 \pmod{32}$ or $2^r + 1 \pmod{2^{r+1}}$, if r is odd, and the few remaining cases can easily be shown impossible.

By the remark after lemma 8 we have $k = \dfrac{F(b, -a)}{d^2} = 109^3 + 9 \cdot 109 \cdot 821^2 - 4 \cdot 821^3$ which is divisible by 13. Now ε^4 (and ε^{-4}) is the least power of ε of the type $13A\varrho^2 + 13B\varrho + C$ and since $A \not\equiv 0 \pmod{13}$, $\varepsilon^n = u + v\varrho$ can have only the solution $n = 0$. Hence the Diophantine equation

$$y^2 - 31 = x^3$$

has exactly one integer solution

$$x = 3, \quad y = \pm 2.$$

$f = 3$ is the first case which gives forms corresponding to other fields.

15. The equations $y^2 - 33f^2 = x^3$

$f = 1$, i.e. *the equation* $y^2 - 33 = x^3$. The reducible form is insoluble and by theorem 5 and conveniant substitutions we get

(1) $$(3, 0, -3, 4) = f = 1$$

(2) $$(1, 0, 6, 10) = f = 1$$

(3) $$(3, 0, 6, 2) = f = 1$$

(4) $$3 \cdot (1, -1, 1, 1) = f = 1$$

which all belong to different fields. (1) is insoluble modulo 9 and corresponds to the ring $R(1, 2\varepsilon, \varepsilon^2 \cdot \varepsilon)$ belonging to the fundamental ring $R(\varepsilon)$ with

(5) $$\varepsilon^3 + 6\varepsilon - 1 = 0$$

and the discriminant -891. (2) corresponds to the fundamental ring $R(\varrho)$ with $\varrho^3-6\varrho-10=0$ and the fundamental unit $\varepsilon=\frac{(\varrho-1)^3}{3}-$ $=-\varrho^2-\varrho+3$, where

$$\varepsilon^3-21\varepsilon^2+111\varepsilon-1=0. \tag{6}$$

Theorem 8 proposes the substitution $\varphi=2\varepsilon-11$, which gives $\varphi^3\equiv$ $\equiv 0 \pmod 9$, and we easily see that

$$(\varphi+11)^n=U+V\varphi^2 \tag{7}$$

only is satisfied by $n=0$, corresponding to $x=-2$.

(3) is insoluble modulo 9 and corresponds as usual to the ring $R(1, \alpha, \beta)$, which is fundamental and has the fundamental unit $\varepsilon=\alpha+1$ with

$$\varepsilon^3-3\varepsilon^2+21\varepsilon-1=0. \tag{8}$$

(4) is of course insoluble and belongs to the field with $D=-44$, where

$$\varepsilon^3+\varepsilon^2+\varepsilon-1=0. \tag{9}$$

Hence the Diophantine equation

$$y^2-33=x^3$$

has exactly one integer solution

$$x=2,\quad y=5.$$

$f=3$, i.e. *the equation* $y^2-297=x^3$. This equation will be of current interest in chapter III. The reducible form is insoluble and putting $f=3$ in (1)—(4) we get by theorem 6 exactly the four forms $(1, 0, -9, 36)=1$, $(1, 0, -36, 90)=1$, $(1, 3, 21, 1)=1$ and $(1, -1, 1, 1)=1$ and by theorem 8 we find that these forms have respectively 1, 1, 2 and 4 solutions. Hence the equation has exactly 8 solutions which are given for $-k=11$ in table 3. The first case which gives forms corresponding to other fields is $f=17$.

16. The equations $y^2-37f^2=x^3$

If f satisfies the conditions of theorem 4 we get only one irreducible form

$$(1, 0, 3, 12)=8f. \tag{1}$$

The fundamental ring of the field has $D=-999$ and is represented by the form $(2, -3, 3, 2)$. This form can only assume even values and is said to have the non-essentiel discriminant divisor (ausserwesentlichen Diskriminantenteiler) 2. That a field contains such a form is a necessary and sufficient condition that the ideal (2) divide into three different ideals in the field (cp Levi [1] III. Satz). We have

Theorem 9. *Suppose k square-free, $h(K\sqrt{k})$ not divisible by 3 and $(2f, x)$ not containing primes which divide into two different ideals in $K(\sqrt{k})$. Then all irreducible forms corresponding to the equation $y^2 - -kf^2 = x^3$ belong to a cubic field with the odd discriminant $-3^{2s-1}\cdot k$ if $k\equiv 1 \pmod 4$, and the even discriminant $-4\cdot 3^{2s-1}\cdot k$, if $k\not\equiv 1 \pmod 4$, $s=0$, 1 or 2. In these fields the ideal (2) divides into three different ideals if and only if $k\equiv 5 \pmod 8$ and the fundamental unit of $K(\sqrt{k})$ is of the type $A+B\sqrt{k}$. Otherwise, if $k\equiv 5 \pmod 8$, (2) is a prime ideal. If $k\equiv 1 \pmod 8$, (2) divides into two different prime ideals. If $k\not\equiv 1 \pmod 4$ we get $(2)=\mathfrak{p}^2\cdot\mathfrak{p}_1$.*

Proof. By theorem 4 we get the irreducible forms from

$$\pm y + f\sqrt{k} = \varepsilon\cdot\alpha^3.$$

$k\not\equiv 1 \pmod 4$ must give forms with D even, since $D\equiv 0$ or $1 \pmod 4$. It is easy to show that $(2)=\mathfrak{p}^3$ is impossible and hence $(2)=\mathfrak{p}^2\cdot\mathfrak{p}_1$. If $k\equiv 5 \pmod 8$ and $\varepsilon = A+B\sqrt{k}$ we get

$$(B, 3A, 3Bk, Ak) = 8f$$

where either $A\equiv 2 \pmod 4$ or $B\equiv 0 \pmod 4$. In both the cases we get

$$(B, 3A, 3Bk, Ak)\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = (B, P, 2Q, 8R)$$

with P and Q odd, and then the field contains the form $(2B, P, Q, 2R)$ with odd discriminant. Then by Levi (2) divides into three different ideals. If $k\equiv 5 \pmod 8$ and $\varepsilon = \dfrac{A+B\sqrt{k}}{2}$ we get in the case $f=4f_1$ $(B, 3A, 3Bk, Ak) = 64f_1$, and $(B, 3A, 3Bk, Ak)\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = (B, 2P, 4Q, 8R)$. Then the form (B, P, Q, R) has $D=-27k$, and the field cannot contain any form $(2a, b, c, 2d)$ with b and c odd, since in this

case all forms with odd discriminant must have this form. Then (2) is a prime ideal (cp Levi p 37, 2. Ergänzungssatz). Finally $k \equiv 1 \pmod 8$ gives $\varepsilon = A + B\sqrt{k}$ with A or $B \equiv 0 \pmod 4$ and we get $(B, 3A, 3Bk, Ak) = f$ and as before $(4a, b, 2c, 4d) = f$ with b, c and d odd. $(8a, b, c, d)$ belongs to the field and has odd discriminant. We easily see that (2) cannot be a prime ideal and hence (2) divides into two prime ideals by the cited Ergänzungssatz.

I have also found in the same way that the three other fields, corresponding to $k \equiv 1 \pmod 8$, $f = 1$ by theorem 5, all have even discriminant and factorize $(2) = \mathfrak{p}^3$, if there is a principle ideal in the quadratic field $K(\sqrt{k})$ with the norm 2. Probably this last restriction is not necessary.

$f = 1$, i.e. *the equation* $y^2 - 37 = x^3$. The reducible form is insoluble and conveniant substitutions transform (1) in the three forms

(2) $\qquad (1, 0, 3, 12) \quad = f = 1$

(3) $\qquad (1, 0, -9, 16) = f = 1$

(4 $\qquad (2, -3, 6, 3) \quad = f = 1.$

(4) defines the ring $R(1, \alpha, \beta)$ and the factorization $(2) = \mathfrak{p} \cdot \mathfrak{p}_1 \cdot \mathfrak{p}_2$, $(3) = \mathfrak{q}^3$, $(\alpha) = \mathfrak{p}^2 \cdot \mathfrak{q}$ and $(1 - \alpha) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ gives the unit $\varepsilon = -44\alpha + 70\beta - 491$, where

(5) $$\varepsilon^3 + 921\varepsilon^2 + 160941\varepsilon - 1 = 0.$$

ε is the fundamental unit of the field as can be shown by Nagell's method. (4) is insoluble by lemma 4, since there is no integer in the ring with the norm 2. (2) defines the ring $R(\theta)$, where $\theta^3 + 3\theta - 12 = 0$. We get $\varepsilon = 13\theta^2 + 127\theta - 281$. The condition $n \geq 0$ and

(6) $$(13\theta^2 + 127\theta - 281)^n = u + v\theta$$

implies $n \equiv 0 \pmod 3$ but this is impossible by lemma 8. Then (2) has only the solution (1, 0), corresponding to $x = -1$.

(3) defines the ring $R(\theta_1)$ with $\theta_1^2 - 9\theta_1 - 16 = 0$ and $\varepsilon = 57\theta_1^2 - 31\theta_1 - 649$. Put at first $\theta_1 = \varphi - 2$ with $\varphi^3 - 6\varphi^2 + 3\varphi - 6 = 0$. Then

$$\varepsilon^n = (57\varphi^2 - 259\varphi - 359)^n = U + V\varphi$$

implies that $n \equiv 0 \pmod 3$, which is impossible by lemma 8, or $n \equiv 4 \pmod{27}$. Now put $\theta_1 = \psi + 1$ with $\psi^3 + 3\psi^2 - 6\psi - 24 = 0$. Then the proposition $n \equiv 4 \pmod 9$ in

$$\varepsilon^n = (57\psi^2 + 83\psi - 623)^n = U_1 + V_1\psi$$

implies that $n \equiv 13 \pmod{27}$, which contradicts the earlier result, and (3) has only the solution (1, 0), corresponding to $x = 3$. Hence the Diophantine equation

$$y^2 - 37 = x^3$$

has exactly the two integer solutions

$$x = -1, \qquad y = \pm 6$$
$$x = 3, \qquad y = \pm 8.$$

Already $f = 3$ gives forms corresponding to other fields.

17. The equations $y^2 - 41f^2 = x^3$

Except the reducible form we get by theorem 5 and after conveniant substitutions

(1) $(2, 3, -6, 5) = f$

(2) $(1, 0, -6, 14) = f$

(3) $(2, 6, 12, 3) = f$

(4) $(2, 6, -6, 3) = f.$

(1) belongs to a field with $D = -27 \cdot 41$ and represented by the form $(3, -3, -3, 4)$ as usual defining the fundamental ring $R(1, \alpha, \beta)$. We get the fundamental unit $\varepsilon = 2\alpha - 2\beta + 1$ with

(5) $$\varepsilon^3 - 3\varepsilon^2 + 27\varepsilon - 1 = 0.$$

(2) belongs to the fundamental ring $R(\varrho)$, defined by the form $(1, -1, 3, 3)$ and with $D = -492$ and the fundamental unit $\varepsilon = 2\varrho^2 - 1$, where

(6) $$\varepsilon^3 + 13\varepsilon^2 + 53\varepsilon - 1 = 0.$$

(3) defines a fundamental ring $R(1, \alpha, \beta)$ with the fundamental unit $\varepsilon = \alpha + \beta - 11$, where

(7) $$\varepsilon^3 + 15\varepsilon^2 + 63\varepsilon - 1 = 0.$$

(4) defines a fundamental ring $R(1, \gamma, \delta)$ with the fundamental unit $\varepsilon = -\gamma + \delta + 7$, where

(8) $$\varepsilon^3 - 9\varepsilon^2 + 39\varepsilon - 1 = 0.$$

$f = 1$, i.e. *the equation* $y^2 - 41 = x^3$. The reducible form is insoluble and so are (1), (3) and (4), which can be seen modulo 9. (2) belongs to the ring $R(\theta)$ with $\theta^3 - 6\theta - 14 = 0$ and the fundamental unit $\varepsilon^2 = 12\theta^2 - 24\theta - 47$, where ε is defined by (6), but then there is only the solution $(1, 0)$ by lemma 8 and the Diophantine equation

$$y^2 - 41 = x^3$$

has exactly one integer solution

$$x = 2, \quad y = \pm 7.$$

The first case giving forms corresponding to other fields is $f = 5$.

18. The equations $y^2 - 43f^2 = x^3$

$f = 1$, i.e. *the equation* $y^2 - 43 = x^3$. The reducible form is insoluble and by theorem 4 we get by a conveniant substitution

(1) $$(1, 0, 9, 8) = f = 1.$$

The corresponding ring $R(\theta)$ belongs to the fundamental ring $R(1, \alpha, \beta)$ with $D = -516$, represented by the form (2, 4, 3, 3) and with the fundamental unit $\varepsilon = 23 - 7\alpha$, where

(2) $$\varepsilon^3 - 41\varepsilon^2 + 593\varepsilon - 1 = 0.$$

$R(\theta)$ has the fundamental unit $\varepsilon^2 = -42\theta^2 + 140\theta - 87$ and then, by lemma 8, (1) has only the solution $(1, 0)$ and the Diophantine equation

$$y^2 - 43 = x^3$$

has exactly one integer solution

$$x = -3, \quad y = \pm 4.$$

Already $f = 3$ gives forms corresponding to other fields.

19. The equations $y^2 - 57f^2 = x^3$

If f contains no odd prime dividing into two different ideals in the quadratic field $K(\sqrt{57})$ we get except the reducible form only the four forms

(1) $$(1, 0, -21, 40) = f$$

(2) $$(1, 0, 6, 14) \quad = f$$

(3) $3 \cdot (1, 1, 3, 1) \cdot \quad = f$

(4) $(1, 0, -12, 22) = f.$

(1) defines the ring $R(\theta)$ with $\theta^3 - 21\theta - 40 = 0$, which belongs to the fundamental ring $R(\varrho)$ with $\varrho^3 + 6\varrho - 5 = 0$ and $D(\varrho) = -3^4 \cdot 19$. $R(\varrho)$ has the fundamental unit $\varepsilon = 2\varrho^2 + 34\varrho - 27$ with

(5) $$\varepsilon^3 + 105\varepsilon^2 + 9543\varepsilon - 1 = 0.$$

(2) defines the fundamental ring $R(\alpha)$ with $\alpha^3 + 6\alpha - 14 = 0$ and the fundamental unit $\varepsilon = \alpha^2 - \alpha - 1$, where

(6) $$\varepsilon^3 + 15\varepsilon^2 + 111\varepsilon - 1 = 0.$$

(3) belongs to the field $K(\varepsilon)$ with $D = D(\varepsilon) = -76$ and

(7) $$\varepsilon^3 - \varepsilon^2 + 3\varepsilon - 1 = 0.$$

(4) defines the fundamental ring $R(\beta)$ with $\beta^3 - 12\beta - 22 = 0$ and the fundamental unit $\varepsilon = -\beta^2 + 2\beta + 9$, where

(8) $$\varepsilon^3 - 3\varepsilon^2 + 39\varepsilon - 1 = 0.$$

$f = 1$, i.e. *the equation* $y^2 - 57 = x^3$. The reducible form is insoluble. In the ring $R(\theta)$, defined by (1), we get $\varepsilon = -16\theta^2 + 50\theta + 189$, where ε is defined by (5). Then theorem 8 proposes the substitution $\varphi = 8\varepsilon + 457$, which gives $\varphi^3 \equiv 0 \pmod 9$, and we easily find that (1) has the only solution (1, 0), corresponding to $x = 7$. In the same way theorem 8 proposes the substitutions $\varphi = 2\varepsilon + 7$ and $\varphi = \varepsilon - 19$ in the cases (2) and (4) respectively and each of these forms has only the solution (1, 0), corresponding to $x = -2$ and 4 resp. (3) is of course insoluble. Hence the Diophantine equation

$$y^2 - 57 = x^3$$

has exactly three integer solutions

$$x = 2, \qquad y = \pm 7$$
$$x = 4, \qquad y = \pm 11$$
$$x = 7, \qquad y = \pm 20.$$

$f = 3$, i.e. *the equation* $y^2 - 513 = x^3$. We will meet this equation in chapter III. The reducible form is insoluble and (1), (2) and (4) give $(2, -9, 18, 9) = 1$, $(2, 12, -12, 7) = 1$ and $(2, 0, 18, 9) = 1$ resp., which all are insoluble modulo 9. (3) gives the three solutions (1, 0),

(0, 1) and (13, −36), corresponding to the solutions for $-k=19$ in table 3.

The first case which gives forms corresponding to other fields is $f=7$.

20. The equations $y^2-65f^2=x^3$

In this case 2^2 is the least power of 2, which is norm of a principal ideal in the quadratic field $K(\sqrt{65})$, and if f contains no odd primes which divide into two different ideals in this field, we get by theorem 5 and after conveniant substitutions a reducible form and

(1) $(1, 0, 3, 16) = f$

(2) $(2, 0, -6, 9) = f$

(3) $(1, 0, 12, 2) = f$

(4) $(1, 12, 6, 2) = f.$

(1) belongs to the fundamental ring $R(1, \alpha, \beta)$, defined by the form $(2, -3, 3, 3)$ with $D=-27\cdot 65$. This ring has the fundamental unit $\varepsilon=-7\alpha^2+7\alpha+1$ with

(5) $$\varepsilon^3-3\varepsilon^2+8235\varepsilon-1=0.$$

(2) belongs to the fundamental ring $R(\varrho)$, where $\varrho^3+2\varrho^2-6=0$ and $D=-780$. The fundamental unit of the field is $\varepsilon=5\varrho^2+3\varrho-13$, where

(6) $$\varepsilon^3+25\varepsilon^2+473\varepsilon-1=0.$$

(3) defines the fundamental ring $R(\gamma)$ with $\gamma^3+12\gamma-2=0$ and the fundamental unit $\varepsilon=1-6\gamma$, defined by

(7) $$\varepsilon^3-3\varepsilon^2+435\varepsilon-1=0.$$

(4) defines the fundamental ring $R(\delta)$ with $\delta^3-12\delta^2+6\delta-2=0$ and the fundamental unit $\varepsilon=3\delta^2-33\delta-17$, defined by

(8) $$\varepsilon^3+51\varepsilon^2+1179\varepsilon-1=0.$$

$f=1$, i.e. *the equation* $y^2-65=x^3$. The reducible form is insoluble and so is (2), which can be seen modulo 9. (1) defines the ring $R(\theta)$ with $\theta^3+3\theta-16=0$ and $\varepsilon=-7\theta^2+21\theta-13$, where ε is defined by (5). Then by lemma 8 (1) has the only solution (1, 0), corresponding to $x=-1$.

Since $D(\varepsilon) \neq D(\gamma)$, (3) has exactly the two solutions (1, 0) and (1, -6), corresponding to $x = -4$ and 584. Finally (4) has the only solution (1, 0) by lemma 8 and the Diophantine equation

$$y^2 - 65 = x^3$$

has exactly the four integer solutions

$$\begin{aligned} x &= -4, & y &= \pm 1 \\ x &= -1, & y &= \pm 8 \\ x &= 14, & y &= \pm 53 \\ x &= 584, & y &= \pm 14113. \end{aligned}$$

The first case, which gives forms corresponding to other fields is $f = 7$.

21. The equations $y^2 - 73f^2 = x^3$

As before theorem 5 after conveniant substitutions gives four irreducible forms

(1) $(1, 0, -9, 20) = f$

(2) $(1, 0, -6, 18) = f$

(3) $(1, 15, 57, 1) = f$

(4) $(1, 0, 12, 6) = f.$

(1) belongs to the fundamental ring $R(1, \alpha, \beta)$ defined by the form (2, 3, -3, 3) with $D = -27 \cdot 73$ and the fundamental unit $\varepsilon = 8\alpha + 50\beta - 101$ with

(5) $$\varepsilon^3 + 429\varepsilon^2 + 63371\varepsilon - 1 = 0.$$

(2) belongs to the fundamental ring $R(1, \gamma, \delta)$ defined by the form (3, 0, -2, 2) with $D = -876$ and the fundamental unit $\varepsilon = 4\gamma - 7\delta - 1$, where

(6) $$\varepsilon^3 - 11\varepsilon^2 + 1839\varepsilon - 1 = 0.$$

(3) defines the fundamental ring $R(\varepsilon)$ with

(7) $$\varepsilon^3 - 15\varepsilon^2 + 57\varepsilon - 1 = 0$$

and (4) defines the fundamental ring $R(\varrho)$ with $\varrho^3 + 12\varrho - 6 = 0$ and the fundamental unit $\varepsilon = 1 - 2\varrho$, where

(8) $$\varepsilon^3 - 3\varepsilon^2 + 51\varepsilon - 1 = 0.$$

$f = 1$, i.e. *the equation* $y^2 - 73 = x^3$. The reducible form is insoluble.

(1) defines the ring $R(\theta)$ with $\theta^3 - 9\theta - 20 = 0$ and $\varepsilon = 25\theta^2 - 17\theta - 293$. $\varepsilon^n = u + v\theta$ must have v even. This implies n even, since $\varepsilon^n = A_n\theta^2 + B_n\theta + C_n$ gives $B_n \equiv \sum_{i=1} \binom{n}{i} \cdot \sum_{k=0} \binom{i}{2k+1} \equiv n \pmod 2$, which easily follows from the function congruence $\theta^i \equiv (i+1)\cdot\theta^2 + i\cdot\theta \pmod 2$, $i \neq 0$. However, n even is impossible by lemma 8, since $\varepsilon^2 \equiv C_2 \pmod 7$ and A_2 is not divisible by 7^2, and then (1) has the only solution (1, 0), corresponding to $x = 3$.

(2) defines the ring $R(\varphi)$ with $\varphi^3 - 6\varphi - 18 = 0$ and the fundamental unit $\varepsilon^2 = -12\varphi^2 + 90\varphi - 167$, where ε is defined by (6). Then, by lemma 8, (2) has the only solution (1, 0) corresponding to $x = 2$.

(3) has exactly the two solutions (1, 0) and (0, 1) which may be shown as before after the substitution $\varepsilon = 5 - \psi$.

(4) has exactly the two solutions (1, 0) and (1, −2) by lemma 1. Hence the Diophantine equation

$$y^2 - 73 = x^3$$

has exactly the six integer solutions

$$\begin{aligned} x &= -4, & y &= \pm 3 \\ x &= 2, & y &= \pm 9 \\ x &= 3, & y &= \pm 10 \\ x &= 6, & y &= \pm 17 \\ x &= 72, & y &= \pm 611 \\ x &= 356, & y &= \pm 6717. \end{aligned}$$

Already $f = 3$ gives forms corresponding to other fields.

22. The equations $y^2 - 82f^2 = x^3$

$f = 1$, i.e. *the equation* $y^2 - 82 = x^3$. Except the insoluble reducible form we get by theorem 4 and after conveniant substitutions

$$(1, 0, 3, 18) = 1. \tag{1}$$

This form defines the ring $R(\theta)$ belonging to the fundamental ring defined by the form (2, 1, 0, 3) and with $D = -984$. We have the factorization $(2) = \mathfrak{p}^2 \cdot \mathfrak{p}_1$ and $(3) = \mathfrak{q}^2 \cdot \mathfrak{q}_1$ and get the unit $\varepsilon = 11\theta^2 + 7\theta - 71$, which by Nagell's method is the fundamental unit of the field and where

(2) $$\varepsilon^3 + 279\,\varepsilon^2 + 21573\,\varepsilon - 1 = 0.$$

The condition $\varepsilon^n = (11\,\theta^2 + 7\,\theta - 71)^n = u + v\,\theta$ with $n \geq 0$ by lemma 7 implies at first that $n \equiv 0 \pmod 3$ but this gives a contradiction modulo 3^{p+2}, if we put $n = 3^p \cdot n_1$. Hence the Diophantine equation

$$y^2 - 82 = x^3$$

has exactly one integer solution

$$x = -1, \qquad y = \pm 9.$$

Already $f = 3$ gives forms corresponding to other fields.

23. The equations $y^2 - 89f^2 = x^3$

As in the earlier cases with $k \equiv 1 \pmod 8$ we get four irreducible forms

(1) $(1, 21, -18, 4) = f$

(2) $(1, 0, 6, 18) \quad = f$

(3) $(1, 9, -3, 3) \quad = f$

(4) $(1, 0, 12, 10) \quad = f.$

(1) belongs to the field, defined by the fundamental ring $R(\varrho)$ with $D = -27 \cdot 89$ and $\varrho^3 - 6\,\varrho - 11 = 0$. The fundamental ring of this field is $\varepsilon = -10\,\varrho^2 + 50\,\varrho - 59$, where

(5) $$\varepsilon^3 + 297\,\varepsilon^2 + 29703\,\varepsilon - 1 = 0.$$

(2) belongs to the fundamental ring $R(1, \alpha, \beta)$, defined by the form (3, 0, 2, 2) and with $D = -1068$. The fundamental unit of this field is $\varepsilon = -3\,\alpha + 9\,\beta - 23$ with

(6) $$\varepsilon^3 + 51\,\varepsilon^2 + 1299\,\varepsilon - 1 = 0.$$

(3) defines the fundamental ring $R(\gamma)$ with $\gamma^3 - 9\,\gamma^2 - 3\,\gamma - 3 = 0$ and the fundamental unit $\varepsilon = -2\,\gamma^2 + 17\,\gamma + 16$, where

(7) $$\varepsilon^3 - 27\,\varepsilon^2 + 273\,\varepsilon - 1 = 0.$$

(4) defines the fundamental ring $R(\delta)$ with $\delta^3 + 12\,\delta - 10 = 0$ and the fundamental unit $\varepsilon = \delta^2 + 3\,\delta - 3$, where

(8) $$\varepsilon^3 + 33\,\varepsilon^2 + 333\,\varepsilon - 1 = 0.$$

$f = 1$, i.e. *the equation* $y^2 - 89 = x^3$. The reducible form is insoluble.

(1) defines the ring $R(\theta)$ with $\theta^3 - 21\,\theta^2 - 18\,\theta - 4 = 0$, where $\varepsilon = 40\,\theta^2 - 850\,\theta - 509$. Then there is only the solution (1, 0) by lemma 8.

(2) defines the ring $R(\varphi)$ with $\varphi^3 + 6\varphi - 18 = 0$ and we get $\varepsilon = 3\varphi^2 - 3\varphi - 5$ and hence the only solution (1, 0) by lemma 8. As before the condition $\varepsilon^n = u + v\gamma$ shows that (3) has the only solution (1, 0) and we get the same result for (4) since $n \geq 0$ by lemma 7. Hence the Diophantine equation

$$y^2 - 89 = x^3$$

has exactly the four solutions

$$\begin{aligned} x &= -4, & y &= \pm 5 \\ x &= -2, & y &= \pm 9 \\ x &= 10, & y &= \pm 33 \\ x &= 55, & y &= \pm 408. \end{aligned}$$

The first case which gives forms corresponding to other fields is $f = 5$.

24. The equations $y^2 - 97f^2 = x^3$

We get the four irreducible forms

(1) $(2, 9, 18, 4) = f$

(2) $(2, 12, 6, 3) = f$

(3) $(1, 12, -6, 2) = f$

(4) $(2, 18, 42, 3) = f.$

(1) belongs to the fundamental ring $R(\varrho)$ with $D = -27 \cdot 97$ and defined by $\varrho^3 - 6\varrho^2 - 6\varrho - 3 = 0$. The fundamental unit of the field is $\varepsilon = 2\varrho^2 - 14\varrho + 1$ with

(5) $$\varepsilon^3 - 15\,\varepsilon^2 + 111\,\varepsilon - 1 = 0.$$

(2) defines the fundamental ring $R(1, \alpha, \beta)$ with the fundamental unit $\varepsilon = \alpha - 11$ and

(6) $$\varepsilon^3 + 21\,\varepsilon^2 + 111\,\varepsilon - 1 = 0.$$

(3) belongs to the fundamental ring $R(1, \gamma, \delta)$ defined by the form $(3, 6, -14, 6)$ with $D = -1164$ and the fundamental unit $\varepsilon = -9\gamma + 9\delta + 79$, where

(7) $$\varepsilon^3 - 57\,\varepsilon^2 + 975\,\varepsilon - 1 = 0.$$

(4) defines the fundamental ring $R(1, \varphi, \psi)$ with the fundamental unit $\varepsilon = 20\varphi + 3\psi - 125$ and

$$\varepsilon^3 - 111\varepsilon^2 + 3741\varepsilon - 1 = 0. \tag{8}$$

$f = 1$, i.e. *the equation* $y^2 - 97 = x^3$. The reducible form is insoluble and so are (1), (2) and (4), which may be seen modulo 9. (3) defines the ring $R(\theta)$, where $\theta^3 - 12\theta^2 - 6\theta - 2 = 0$, and we get $\varepsilon = 3\theta^2 - 39\theta + 19$, i.e. (3) has the only solution (1, 0) by lemma 8. Hence the Diophantine equation

$$y^2 - 97 = x^3$$

has exactly one integer solution

$$x = 18, \qquad y = \pm 77.$$

Already $f = 3$ gives forms corresponding to other fields.

25. The remaining cases with $0 < kf^2 < 100$

The equation $y^2 - 74 = x^3$. By theorem 4 we have to examine the form

$$(4, 3, 6, 5) = 1$$

which is insoluble modulo 9. Hence the equation is insoluble.

The equation $y^2 - 79 = x^3$. Since $h(K(\sqrt{79}))$ is 3 and $3^3 = (17 + 2\sqrt{79}) \cdot (17 - 2\sqrt{79})$ is the least power of 3 dividing into principle ideals we get by theorem 4 the four irreducible forms

$$(1, 21, 12, 2) = 1$$
$$(2, -3, 6, 6) = 1$$
$$(2, 0, 9, 5) = 1$$
$$(2, 3, -6, 7) = 1$$

all corresponding to different fields. The last three forms are all insoluble modulo 9. The first form defines the ring $R(\theta)$ with $\theta^3 - 21\theta^2 + 12\theta - 2 = 0$. $R(\theta)$ belongs to the fundamental ring $R(\varrho)$ with $\varrho^3 + \varrho^2 - 6 = 0$ and $D = -948$ and with the fundamental unit $\varepsilon = 17\varrho^2 - 45\varrho + 29$, where

$$\varepsilon^3 - 149\varepsilon^2 + 23357\varepsilon - 1 = 0.$$

$R(\theta)$ has the fundamental unit $\varepsilon^2 = -8634\theta^2 + 179412\theta - 63929$ and

then the form has the only solution (1, 0) by lemma 8 and the equation

$$y^2 - 79 = x^3$$

has exactly one integer solution

$$x = 45, \qquad y = \pm 302.$$

Further I have theoretically solved all the equations with $kf^2 = 22$, 26, 30, 35, 38, 71, 92 and 94 by giving upper limits for the eventually remaining solution. I have determined a unit ε in the corresponding ring and shown that 1) if $\varepsilon = \eta^m$, $m > 1$, then η must be of the type $u + v\theta$ and give a second solution of the equation and 2) if ε is the fundamental unit, then the equation has no solution more. Then the limit for $|v|$ given by Nagell's method is a limit for possible solutions of the form $F(u, v) = 1$. By Nagell [6] Satz XXII we have $v^6 \leq \frac{1}{4} \cdot \frac{D(\varepsilon)}{D(\theta)}$. Of course this gives a very great upper limit for the solutions (x, y) of $y^2 - kf^2 = x^3$, e.g. $x < 1.56 \cdot 10^7$ in the case $y^2 - 26 = x^3$, which probably gives the least value. In the results stated below θ is defined by the given form.

The equations $y^2 - 22f^2 = x^3$. $f = 1$ gives the form $(1, 0, -9, 14) = 1$ and we get $\varepsilon = \frac{(-5\theta^2 + 11\theta - 25)^3}{9} = -185\theta^2 + 609\theta - 199$ and $|v| < 1993$ $(m \geq 11)$.

The equations $y^2 - 23f^2 = x^3$. The first soluble case is $f = 2$, i.e. the equation $y^2 - 92 = x^3$. We get the forms $(1, 0, -6, 20) = 1$, defining the ring $R(\alpha)$ and belonging to the fundamental ring $R(1, \alpha, \beta) = R\left(1, \alpha, \frac{\alpha^2}{2}\right)$, defined by the form $(2, 0, -3, 5)$, and $(2, 3, 12, 3) = 1$, defining a ring $R(1, \gamma, \delta)$. This last form is insoluble, since $\lambda = \mathfrak{p}_1$ is no principle ideal of the ring. $(2) = \mathfrak{p}^2 \cdot \mathfrak{p}_1$. We get $\varepsilon = \frac{(5\alpha + 2\beta - 23)^3}{9} = 68\alpha^2 + 965\alpha - 4121$ and $|v| < 3513$.

The equations $y^2 - 26f^2 = x^3$. $f = 1$ gives the form $(1, 0, 3, 10) = 1$, $\varepsilon = \frac{(-\theta^2 + 7\theta - 9)^3}{3} = -281\theta^2 - 651\theta + 1917$ and $|v| < 1013$.

The equations $y^2 - 30f^2 = x^3$. $f = 1$ gives the form $(1, 0, -57, 166) = 1$, $\varepsilon = \frac{(-\theta^2 + 7\theta + 15)^3}{3} = -1349\theta^2 + 6913\theta + 42293$ and $|v| < 4225$.

The equations $y^2-35f^2=x^3$. $f=1$ gives the form $(1, 0, -3, 12)=1$ and $\varepsilon=-1343\theta^2-15347\theta-31823$ and we get $|v|<17740$.

The equations $y^2-38f^2=x^3$. $f=1$ gives the form $(1, 0, -33, 74)=1$, $\varepsilon=\dfrac{(-11\theta^2-35\theta-253)^3}{9}=539\theta^2-1177\theta-15971$ and $|v|<987$.

The equations $y^2-71f^2=x^3$. $f=1$ gives the form $(1, 0, -15, 28)=1$ and $\varepsilon=\dfrac{(2\theta^2-2\theta-33)^3}{3}=562\theta^2-1290\theta-5931$ and we get $|v|<1719$.

The equations $y^2-94f^2=x^3$. $f=1$ gives the form $(1, 0, -9, 22)=1$ and $\varepsilon=\dfrac{(3\theta^2-5\theta-25)^3}{3}=-361\theta^2-131\theta+5821$ and we get $|v|<1813$.

In the remaining cases 55 and 91 my calculated units are larger and I surrender determining any limit. $y^2-55=x^3$ gives $(1, 0, -27, 56)=1$ and the unit $\varepsilon=\dfrac{(25\theta^2-97\theta-323)^3}{9}$ and $y^2-91=x^3$ gives $(1, 0, 9, 16)=1$ and the unit $\varepsilon=\dfrac{(-23\theta^2-167\theta+289)^3}{9}$.

26. Some equations with $k<0$

If $k<0$ all corresponding irreducible forms have a positive discriminant and belong to cubic fields, where we have two fundamental units. I shall state the solutions of one such form below but generally this problem is much more difficult. However, as remarked after theorem 4, we get only reducible forms from $y^2-kf^2=x^3$, if f contains no primes dividing in two different ideals in $K(\sqrt{k})$, $h(K(\sqrt{k}))$ is not divisible by 3 and $k\neq -3$. This gives the result: The equations

$$y^2-56=x^3 \text{ and } y^2+84=x^3$$

are both insoluble. The equations

$$y^2-20=x^3,\ y^2-40=x^3 \text{ and } y^2+54=x^3$$

have each exactly one integer solution, namely $(6, \pm 14)$, $(14, \pm 52)$ and $(7, \pm 17)$ resp.. $h(K(\sqrt{-83}))$ is divisible by 3 and since $N\left(\dfrac{5-\sqrt{-83}}{2}\right)=27$ we get by theorem 4

$$(1, 0, -9, 5)=2$$

but this is impossible modulo 9 and the equation

$$y^2 - 83 = x^3$$

has only the solution $x = 27$, $y = \pm 140$ from the reducible form.

In the case $k = -3$, $f = 4$, i.e. *the equation* $y^2 + 48 = x^3$ we get the form

$$(1, 0, -3, 1) = 1 \tag{1}$$

defining the cubic field with $D = 81$. Ljunggren [1] has shown that (1) has exactly the six integer solutions (1, 0), (0, 1), $(-1, -1)$, (1, 3), $(-3, -2)$ and $(2, -1)$. The three first solutions correspond to $x = 4$, $y = \pm 4$ and the three latter solutions to $x = 28$, $y = \pm 148$. Since the reducible form is insoluble, the equation has exactly these two solutions.

Cassels has shown that the equation $y^2 + 31 = x^3$ is insoluble ([1] § 15).

In all the 22 undecided cases with $-kf^2 \leq 100$ (see table 2) we get soluble irreducible forms with positive discriminant.

III

The equations $y^2 + 27k = x^3$

When $k \neq 0$ the function $y^2 - k = x^3$ is geometrically a cubic curve of genus 1 and the substitution

$$x = \wp u, \quad y = \tfrac{1}{2}\wp' u$$

transforms the equation to the Weierstrassian normal form

$$(\wp' u)^2 = 4(\wp u)^3 + 4k$$

i.e. the curve is described by the elliptic function $\wp(u; 0, -4k)$. By complex multiplication of the parameter u by $\sqrt{-3}$ we get the relation

$$\wp(u; 0, 4 \cdot 27k) = \frac{\wp^3(u; 0, -4k) + 4k}{\wp^2(u; 0, -4k)}$$

c.p. Billing [1] Satz 1, p 58. This shows the interdependence between the equations

$$y^2 - k = x^3 \tag{1}$$

and

$$Y^2 + 27k = X^3 \tag{2}$$

which has been known for a long time and which has been expressed by Fueter [1] in the formulas

$$X = \frac{1}{x^2}(y^2 + 3k) = \frac{x^3 + 4k}{x^2}$$
$$Y = \frac{y}{x^3}(y^2 - 9k) = \frac{y(x^3 - 8k)}{x^3}. \tag{3}$$

For the rational points on a cubic curve of genus 1, if any exist, we have the following theorem by Mordell [3].

Theorem 10. *The values of the parameter u which correspond to rational points on a cubic curve of genus 1 constitute a module with a finite basis $u_1, u_2, \ldots, u_N$.*

Hence every rational point (x, y) on the curve may be expressed

$$x = \wp(m_1 u_1 + m_2 u_2 + \cdots + m_N u_N)$$
$$y = \tfrac{1}{2}\wp'(m_1 u_1 + m_2 u_2 + \cdots + m_N u_N).$$

The rang N of the module is also called the rang of the curve.

When the parameter u for a rational point is a fraction $\frac{\omega}{n}$ of a primitive period ω of $\wp u$ we say that the point is of the finite order n. Otherwise the point is of infinite order. We have the following theorem by Fueter.

Theorem 11. *Solutions of $y^2 - k = x^3$ with $x = 0$ or $y = 0$ are of order 3 and 2 respectively. If k is 6-powerfree the only other solutions of finite order are the two following*

$$k = 1: \quad x = -2, \quad y = \pm 3 \quad \text{and}$$
$$k = -2^4 \cdot 3^3: \quad x = 12, \quad y = \pm 36$$

of order 6 and 3 respectively.

Further we have

Theorem 12. (Billing, c.p. [1] p. 58, Satz 2). *Except in two cases it is possible to select a basis $u_1, u_2, \ldots, u_N$ of the parameters u corresponding to the rational points on the curve (1) such that a similar basis $U_1, U_2, \ldots, U_N$ for the curve (2) is defined by*

$$U_i = \frac{u_i}{3^{\varepsilon_i}}$$

where $\varepsilon_i = 1$ or 0 according to whether $\wp\left(\frac{u_i}{3};\ 0,\ 4 \cdot 27\, k\right)$ is rational or not.

The two exceptions are

1. $k = -3c^2$ and u_i all of infinite order. In this case we get the further basis element $U_{N+1} = \frac{\omega}{3}$, where ω is the lowest real period of $\wp(u;\ 0,\ 4 \cdot 27\, k)$.

2. $k = c^2$, c not a cube. In this case there is an element (say u_N) of finite order which has no correspondence on (2). Moreover if c is a cube and hence u_N of order 6 we get U_N of order 2. In the cases 1 and 2 the rang of (2) is $N+1$ and $N-1$ respectively.

Billing has calculated a basis for each of the curves (1) with $0 < |k| \leq 25$ ([1] table 2). Cassels has extended this examination to

$0 < |k| < 50$ ([1] table 1) but he has restricted himself to determining points corresponding to a system of independent parameters u of infinite order without showing that they are basis points. Using Cassels' table, however, we can state the relation between the basis of (1) and (2) by theorem 12. We have $N \leq 2$ in all these cases with $|k| < 50$. By Billing (p. 59) we can select the basis u_1, u_2 in the following way. Let u_1', u_2' be a basis of (1) and put

$$u_1 = u_1 - \varkappa_1 \omega$$
$$u_2 = u_2' - \varkappa_2 u_1' - \varkappa_3 \omega$$

where $\varkappa = 0$, 1 or -1. Then we have to examine, whether any of these values make $\wp\left(\frac{u_i}{3}; 0, 4 \cdot 27\, k\right)$ rational. If $N = 1$ we can choose an arbitrary parameter u of the module instead of u_1', if only $\wp\left(\frac{u}{3}; 0, 4\,k\right)$ is irrational. Even when $N = 2$ we can choose the values of the table, because $\frac{u_2}{3}$ corresponds to a rational point on (2) but not on (1) (except for $k = 17$, but then u_1, u_2 is a basis). By the addition formula for the function $\wp(u; 0, g)$ and if we denote $\wp u_i = X_i$ and $\wp\left(\frac{u_i}{3}\right) = \xi$ we get

$$X_i = \frac{(\xi^3 - g)^3 - 27\, g\, \xi^6}{9\, \xi^2 (\xi^3 - g)^2}$$

and then $g = 108\, k$ gives

$$\xi^9 - 3^2 X_i \xi^8 - 2^5 3^4 k \xi^6 - 2^3 3^5 k X_i \xi^5 - 2^4 3^7 k^2 \xi^3 - 2^4 3^8 k^2 X_i \xi^2 - \\ - 2^6 3^9 k^3 = 0. \tag{4}$$

We have to examine X_1 and the three values $\wp(u_2 - \varkappa u_1)$ for X_2.

We remind of some elementary definitions from the theory of p-adic numbers. A rational number $\frac{a}{b}$, where a and b are relatively prime rational integers, is a p-adic unit if $p \nmid a\, b$. Every rational number can be written in the form $p^r \cdot E$, where E is a p-adic unit. r is called the order of the p-adic number. If $r \geq 0$ the number is a p-adic integer, if $r < 0$ it is a p-adic fraction. That a p-adic number ξ is of order r can also be denoted

$$\xi \equiv p^r \pmod{p^{r+1}}\,(p).$$

To find out whether there is a rational root ξ in (4) we have the following necessary conditions, which easily can be verified:

1. If X_i is a duadic unit then ξ must be a duadic unit (or possibly a duadic integer of order 2 if $k \equiv 1 \pmod 4$).

$X_i \equiv 0 \pmod 2$ (2) implies that $X_i \equiv 2 \pmod 4$ (2), $k \equiv 0 \pmod 4$ and $\xi \equiv 2 \pmod 4$ (2). X_i is a duadic fraction in the cases $k = -15$, -39, -43, -47, 11, 39, 46 and 47. In all these cases we get X_i of order -2. Then ξ must be of order -2 or possibly of order 2, if k is odd, and of order 1, if k is even (i.e. $= 46$).

2. If X_i is a 3-adic integer, then ξ must be a 3-adic integer of order 1, if $3 \nmid k$. ξ can not be rational if $3 | k$ but $3^3 \nmid k$.

When X_i is a 3-adic fraction it is always of order -2 except X_2 in the case $k = -47$ which is of order -4. X_i of order -2 implies that ξ is a 3-adic unit or possibly of order 1 if $3 \nmid k$ and of order 2 if $3 | k$. The case $k = -47$, where X_i is of order -4, implies that ξ is of order 1 or -2.

3. If X_i is a p-adic integer, $p \neq 2$ or 3, then ξ must be a p-adic unit, except if X_i is a unit and $p^2 | k$, when ξ must be of order 1.

If X_i is a p-adic fraction it must be of even order. In all the actual cases we get the order -2. Since $p^2 \nmid k$ ξ must be a unit or be of order 1 or -2.

By these conditions only few rational values for ξ are possible and they can easily be examined. It is easy to see that $\wp\left(\frac{u_i}{3};\ 0,\ -4k\right)$ is irrational in all the cases where $\wp\left(\frac{u_i}{3};\ 0,\ 108k\right)$ is rational, since we get rational integer points on (2) which cannot correspond to rational points on (1). By (1) and (3) we get a solution (X, Y) of (2) from a solution (x, y) of (1) defined by

$$x^3 - X x^2 + 4k = 0$$

and

$$y^3 - Y y^2 - 9k y + k Y = 0.$$

Hence x and y must be algebraic integers of at most third degree to give a solution (X, Y) in rational integers. If the rational points on (2) have a basis which is contained in a basis of (1), x and y must of course be rational integers and then the necessary and sufficient condition $x^2 | 4k$ easily gives all the integer solutions of (2). In all other cases we get further integer solutions. I have solved 14 of these equations completely by the earlier methods of this paper but 11 of them still remain. The results are given in table 3.

Table 1

k	N	Solutions	Ch II mom.	k	N	Solutions	Ch II mom.
1	3	(−1, 0), (0, 1), (2, 3)		44	2	(−2, 16), (5, 13)	8
2	1	(−1, 1)		48	1	(1, 7)	3
3	1	(1, 2)		49	1	(0, 7)	
4	1	(0, 2)		50	1	(−1, 7)	2
5	1	(−1, 2)		52	1	(−3, 5)	9
8	4	(−2, 0), (1, 3), (2, 4), (46, 312)	2	54	1	(3, 9)	5
				55	≤2	(9, 28)	25
9	5	(−2, 1), (0, 3), (3, 6), (6, 15), (40, 253)		56	1	(2, 8)	10
				57	3	(−2, 7), (4, 11), (7, 20)	19
10	1	(−1, 3)	7	63	[1]	(−3, 6), (1, 8)	6
12	2	(−2, 2), (13, 47)	3	64	3	(−4, 0), (0, 8), (8, 24)	1
15	2	(1, 4), (109, 1138)	11	65	4	(−4, 1), (−1, 8), (14, 53), (584, 14113)	20
16	1	(0, 4)					
17	8	(−2, 3), (−1, 4), (2, 5), (4, 9), (8, 23), (43, 282), (52, 375), (5234, 378661)		68	2	(−4, 2), (152, 1874)	12
				71	<2	(5, 14)	25
				72	1	(−2, 8)	2
				73	6	(−4, 3), (2, 9), (3, 10), (6, 17), (72, 611) (356, 6717)	21
18	1	(7, 19)	2				
19	1	(5, 12)	13				
22	<2	(3, 7)	25	74	0		25
24	4	(−2, 4), (1, 5), (10, 32), (8158, 736844)	5	76	[2]	(−3, 7)	13
				79	1	(45, 302)	25
25	1	(0, 5)		80	4	(−4, 4), (1, 9), (4, 12), (44, 292)	4
26	≤2	(−1, 5)	25				
27	1	(−3, 0)		81	1	(0, 9)	1
28	2	(−3, 1) (2, 6)	6	82	1	(−1, 9)	22
30	≤2	(19, 83)	25	89	4	(−4, 5), (−2, 9), (10, 33), (55, 408)	23
31	1	(−3, 2)	14				
33	1	(−2, 5)	15	91	≤2	(−3, 8)	25
35	≤2	(1, 6)	25	92	≤2	(2, 10)	25
36	4	(−3, 3), (0, 6), (4, 10), (12, 42)	1	94	<2	(3, 11)	25
				97	1	(18, 77)	24
37	2	(−1, 6), (3, 8)	16	98	1	(7, 21)	2
38	≤2	(11, 37)	25	99	1	(1, 10)	8
40	1	(6, 16)	7	100	6	(−4, 6), (0, 10), (5, 15), (20, 90), (24, 118), (2660, 137190)	1
41	1	(2, 7)	17				
43	1	(−3, 4)	18				

[1] See p. 60.

[2] See p. 73.

Table 2

k	N	Solutions	Ch II mom.	k	N	Solutions	Ch II mom.
1	1	(1, 0)		48	2	(4, 4), (28, 148)	26
2	1	(3, 5)		49	1	(65, 524)	
4	2	(2, 2), (5, 11)		53	≥ 1	(9, 26)	
7	≥ 1	(2, 1)		54	1	(7, 17)	26
8	1	(2, 0)		55	≥ 1	(4, 3)	
11	2	(3, 4), (15, 57)		56	0		26
13	1	(17, 70)		60	≥ 1	(4, 2)	
15	≥ 1	(4, 7)		61	≥ 1	(5, 8)	
18	≥ 1	(3, 3)		63	≥ 1	(4, 1)	
19	1	(7, 18)		64	1	(4, 0)	
20	1	(6, 14)	26	67	1	(23, 110)	
23	≥ 1	(3, 2)		71	≥ 1	(8, 21)	
25	≥ 1	(5, 10)		72	≥ 1	(6, 12)	
26	≥ 2	(3, 1), (35, 207)		74	1	(99, 985)	
27	1	(3, 0)		76	2	(5, 7), (101, 1015)	
28	≥ 2	(4, 6), (37, 225)		79	> 1	(20, 89)	
31	0			81	1	(13, 46)	
35	1	(11, 36)		83	1	(27, 140)	26
39	≥ 2	(4, 5), (10, 31)		84	0		26
40	1	(14, 52)	26	87	≥ 1	(7, 16)	
44	1	(5, 9)		89	≥ 1	(5, 6)	
45	1	(21, 96)		95	≥ 1	(6, 11)	
47	≥ 2	(6, 13), (63, 500)		100	≥ 3	(5, 5), (10, 30), (34, 198)	

N is the number of solutions with $y \geq 0$.

All cases shown insoluble by Mordell [1] or earlier are excluded in the tables 1 and 2.

Table 3

k	Basis	N	Solutions	k	Basis	N	Solutions
1	$\frac{\omega}{2}$	1	[3, 0]	1	$\frac{\omega}{2}$	1	[−3, 0]
2	u_1	1	(7, 17)	2	$\frac{u_1}{3}$	1	[3, 9]
3	u_1	1	(13, 46)				
5	$\frac{u_1}{3}$	≥ 3	(6, 9), (19, 82), (24, 117)	3	$\frac{\omega}{3}$	1	[0, 9]
8	$u_1, \frac{\omega}{2}$	3	[6, 0], (10, 28), (33, 189)	4	$\frac{u_1}{3}$	4	[−3, 9], (−2, 10), (6, 18), (366, 7002)
9	u_1	1	(7, 10)	7	u_1	1	[−5, 8]
10	u_1	1	(39, 243)	8	$\frac{\omega}{2}$	1	[−6, 0]
11	u_1	0					
12	u_1	1	(10, 26)	11	$\frac{u_1}{3}, \frac{u_2}{3}$	8	[illegible] (18, 4, 19), (12, 45), (34, 199), (48, 333), (93844, 28748141)
15	$u_1, \frac{u_2}{3}$	≥ 2	(9, 18), (61, 476)				
16	$\frac{\omega}{3}$	1	[12, 36]				
17	u_1, u_2	3	(15, 54), (19, 80), (67, 548)	12	$\frac{\omega}{3}$	1	[0, 18]
18	u_1	0		13	[illegible]		
19	u_1	0		14	[illegible]		
22	u_1	0		18	u_1	1	[−5, 19]
24	$u_1, \frac{u_1+u_2}{3}$	≥ 5	(9, 9), (18, 72), (22, 100), (54, 396), (97, 955)	19	$\frac{u_1}{3}$	3	[−8, 1], (6, 27), [illegible] 887041]
				20	$\frac{u_1}{3}$	2	[−6, 18], (21, 99)
26	u_1	1	(103, 1045)	21	[illegible]		
27	$\frac{\omega}{2}$	1	[9, 0]	22	$\frac{u_1}{3}$	≥ 2	15, 68
28	u_1	1	(30, 162)	24	[illegible]		
30	u_1	0		25	u_1	1	[1, 26]
31	u_1	0					
33	u_1	1	(31, 170)	26	$u_1, \frac{u_2}{3}$	2	[3, 27], [139, 1639]
35	u_1	1	(141, 1674)				
36	u_1	1	(13, 35)	27	[illegible]	2	[illegible] 27], [−8, 1]
37	$u_1, \frac{u_1+u_2}{3}$	≥ 4	(10, 1), (12, 27), (40, 251), (147, 1782)	28	u_1	1	[−3, 27]
38	u_1	0		29	$\frac{u_1}{3}$	1	[1, 28]
39	u_1	0					

Table 3 (Cont.)

k	Basis	N	Solutions
40	u_1	0	
41	u_1	1	(43, 280)
43	$u_1, \frac{u_2}{3}$	≤ 1	(21, 90)
44	u_1	1	(42, 270)
46	u_1	0	
47	u_1	0	
48	u_1	1	(193, 2681)
50	$\frac{u_1}{3}$	≤ 2	(15, 45), (199, 2807)
30	$\frac{u_1}{3}$	≤ 2	(−9, 9)
35	$\frac{u_1}{3}$	2	(−6, 27), (16 71)
38	$\frac{u_1}{3}$	1	(7, 37)
39	$u_1, \frac{u_1+u_2}{3}$	≤ 4	(−9, 18), (27, 144)
40	$\frac{u_1}{3}$	≤ 2	(6, 36)
43	$\frac{u_1}{3}$	1	(4, 35)
44	$\frac{u_1}{3}$	2	(−8, 26), (12, 54)
45	u_1	0	
47	$u_1, \frac{u_2}{3}$	≤ 4	(3, 36), (111, 1170)
48	$u_1, \frac{u_2}{3}$	4	(−8, 28), [0, 36], (9, 45), (72, 612)
49	$\frac{u_1}{3}$	1	(−3, 36)
50	$\frac{u_1}{3}$	1	(−5, 35)

u_i correspond to the rational solutions of $y^2 - k = x^3$ given in Cassels' table.

N is the number of integer solutions of $y^2 + 27\ k = x^3$ with $y \geq 0$. In the excluded cases neither $y^2 - k = x^3$ nor $y^2 + 27\ k = x^3$ have rational solutions.

Solutions in [ ] are of finite order.

Table 4

k	$-D$	Fundamental ring and unit	
2	216	(1, 0, 3, 2)	$\varepsilon = -\varrho^2 - \varrho + 1$
3	324	(1, 0, −3, 4)	$\varepsilon = \varrho^2 + \varrho - 7$
5	135	(1, 0, 3, 1)	$\varepsilon = \varrho$
6	648	(2, 0, 3, 2)	$\varepsilon = \alpha - 1$
7	756	(2, 0, −3, 3)	$\varepsilon = 11\alpha - 6\beta - 23$
10	1080	(1, 0, 3, 6)	$\varepsilon = -21\varrho^2 - 11\varrho + 49$
11	11 · 108	(2, 0, 3, 3)	$\varepsilon = -2\alpha + 24\beta - 95$
13	351	(1, 3, 6, 1)	$\varepsilon = \varrho$
14	14 · 108	(2, 0, −3, 4)	$\varepsilon = -63\alpha - 8\beta + 227$
15	15 · 108	(1, 0, −3, 8)	$\varepsilon = 5 - 2\varrho$
17	459	(1, 0, −6, 7)	$\varepsilon = 2\varrho^2 - 2\varrho - 11$
	17 · 108	(1, 0, −6, 10)	$\varepsilon = \varrho - 3$
	204	(1, 1, 1, 3)	$\varepsilon = -\varrho^2 + \varrho + 1$
	17 · 108	(1, 0, 6, 6)	$\varepsilon = \varrho - 1$
19	19 · 108	(1, 0, −15, 24)	$\varepsilon = -36\varrho^2 + 202\varrho - 179$
21	567	(1, 0, −3, 5)	$\varepsilon = -\varrho^2 + \varrho + 3$
22[1]	22 · 108	(1, 0, −9, 14)	$\varepsilon = 185\varrho^2 - 609\varrho - 199$
23[1]	23 · 108	(2, 0, −3, 5)	$\varepsilon = 965\alpha + 136\beta - 3713$
26[1]	26 · 108	(1, 0, 3, 10)	$\varepsilon = -281\varrho^2 - 651\varrho + 1917$
29	783	(1, −1, 2, 1)	$\varepsilon = \varrho$
30[1]	30 · 108	(1, 0, −57, 166)	$\varepsilon = -1349\varrho^2 + 6913\varrho + 42293$
31	31 · 108	(1, 0, 9, 4)	$\varepsilon = 821\varrho^2 + 109\varrho - 203$
33	891	(1, 0, 6, 1)	$\varepsilon = \varrho$
	33 · 108	(1, 0, 6, 10)	$\varepsilon = -\varrho^2 - \varrho + 3$
	44	(1, −1, 1, 1)	$\varepsilon = \varrho$
	33 · 108	(3, 0, 6, 2)	$\varepsilon = \alpha - 1$
35[1]	35 · 108	(1, 0, −3, 12)	$\varepsilon = -1343\varrho^2 + 15347\varrho - 31823$
37	999	(2, 3, 3, 4)	$\varepsilon = 140\alpha + 26\beta - 473$
38[1]	38 · 108	(1, 0, −33, 74)	$\varepsilon = 539\varrho^2 - 1177\varrho - 15971$
41	27 · 41	(3, −3, −3, 4)	$\varepsilon = 2\alpha - 2\beta + 1$
	492	(1, −1, 3, 3)	$\varepsilon = 2\varrho^2 - 1$
	108 · 41	(2, 6, 12, 3)	$\varepsilon = \alpha + \beta - 11$
	108 · 41	(2, 6, −6, 3)	$\varepsilon = -\alpha + \beta + 7$

[1] ε not definitely proved to be fundamental (c.p. Chapter II, mom. 25).

The form $(1, p, q, r)$ or (a, b, c, d) defines the fundamental ring $R(\varrho)$ or $R(1, \alpha, \beta)$ resp. as before in the paper. D is the discriminant of the field.

Table 4 (Cont.)

k	$-D$	Fundamental ring and unit	
43	516	(2, 4, 3, 3)	$\varepsilon = 23 - 7\alpha$
55[1]	$108 \cdot 55$	(1, 0, −27, 56)	$\varepsilon = \frac{1}{9}(25\varrho^2 - 97\varrho - 323)^3$
57	$27 \cdot 57$	(1, 0, 6, 5)	$\varepsilon = 2\varrho^2 + 34\varrho - 27$
	$108 \cdot 57$	(1, 0, 6, 14)	$\varepsilon = \varrho^2 - \varrho - 1$
	76	(1, 1, 3, 1)	$\varepsilon = \varrho$
	$108 \cdot 57$	(1, 0, −12, 22)	$\varepsilon = -\varrho^2 + 2\varrho + 9$
65	$27 \cdot 65$	(2, −3, 3, 3)	$\varepsilon = 28\alpha - 14\beta + 43$
	780	(1, −2, 0, 6)	$\varepsilon = 5\varrho^2 + 3\varrho - 13$
	$108 \cdot 65$	(1, 0, 12, 2)	$\varepsilon = 1 - 6\varrho$
	$108 \cdot 65$	1, 12, 6, 2)	$\varepsilon = 3\varrho^2 - 33\varrho - 17$
71[1]	$108 \cdot 71$	(1, 0, −15, 28)	$\varepsilon = 562\varrho^2 - 1290\varrho - 5931$
73	$27 \cdot 73$	(2, 3, −3, 3)	$\varepsilon = 8\alpha + 50\beta - 101$
	876	(3, 0, −2, 2)	$\varepsilon = 4\alpha - 7\beta - 1$
	$108 \cdot 73$	(1, 15, 57, 1)	$\varepsilon = \varrho$
	$108 \cdot 73$	(1, 0, 12, 6)	$\varepsilon = 1 - 2\varrho$
79	948	(1, −1, 0, 6)	$\varepsilon = 17\varrho^2 - 45\varrho + 29$
	$108 \cdot 79$	(2, −3, 6, 6)	
	$108 \cdot 79$	(2, 0, 9, 5)	
	$108 \cdot 79$	(2, 3, −6, 7)	
82	984	(2, 1, 0, 3)	$\varepsilon = 33\alpha + 7\beta - 104$
89	$27 \cdot 89$	(1, 0, −6, 11)	$\varepsilon = -10\varrho^2 + 50\varrho - 59$
	1068	(3, 0, 2, 2)	$\varepsilon = -3\alpha + 9\beta - 23$
	$108 \cdot 89$	(1, 9, −3, 3)	$\varepsilon = -2\varrho^2 + 17\varrho + 16$
	$108 \cdot 89$	(1, 0, 12, 10)	$\varepsilon = \varrho^2 + 3\varrho - 3$
91[1]	$108 \cdot 91$	(1, 0, 9, 16)	$\varepsilon = \frac{1}{9}(-23\varrho^2 - 167\varrho + 289)^3$
94[1]	$108 \cdot 94$	(1, 0, −9, 22)	$\varepsilon = -361\varrho^2 - 131\varrho + 5821$
97	$27 \cdot 97$	(1, 6, −6, 3)	$\varepsilon = 2\varrho^2 - 14\varrho + 1$
	$108 \cdot 97$	(2, 12, 6, 3)	$\varepsilon = \alpha - 11$
	1164	(3, 6, −14, 6)	$\varepsilon = -9\alpha + 9\beta + 79$
	$108 \cdot 97$	(2, 18, 42, 3)	$\varepsilon = 20\alpha + 3\beta - 125$

[1] ε not definitely proved to be fundamental (c.p. Chapter II, mom. 25).

Bibliography

Berwick, W. E. H. [1] *The classification of ideal numbers that depend on a cubic irrationality.* (Proc. London Math. Soc. vol. 12, 1913.)

Billing, G. [1] *Beiträge zur arithmetischen Theorie der ebenen kubischen Kurven vom Geschlecht Eins.* (Nova Acta Soc. Sci. Upsal. IV, Bd 11:1, 1938.)

Brauer, A. [1] *Über einige spezielle diophantische Gleichungen.* (Math. Zeitschr. Bd 25, 1926.)

Cassels, J. W. S. [1] *The rational solutions of the Diophantine equation* $Y^2 = X^3 - D$. (Acta Math. Bd 82, 1950.)

Dedekind, R. [1] *Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern.* (J. f. Math. 121, 1900 or Ges. Math. Werke, Vol. II, pp. 148—234, 1930.)

Delaunay, B. [1] *Représentation d'un nombre entier par une forme cubique à discriminant négatif.* (C. R. Acad. Sc., Paris, t. 171, 1920, p. 336 et t. 172, 1921, p. 434.) [2] *Sur des formes binaires cubiques à discriminant négatif.* (Ibid., t. 178, 1924, p, 1458.) [3] *Lösung des Äquivalenzproblems und Tabularisierung der binären kubischen Formen von negativen Discriminante.* (In Russian, Journ. Soc. Phys.-Math. Léningrade, t. 1, fasc. 1, 1926.) [4] *Über den Algorithmus der Erhöhung.* (Ibid. t. 1, fasc. 2, 1927.) [5] *Vollständige Lösung der unbestimmten Gleichung* $X^3 q + Y^3 = 1$ *in ganzen Zahlen.* (Math. Zeitschr. Bd 28, 1928.) [6] *Über die Darstellung der Zahlen durch die binären kubischen Formen von negativer Diskriminante.* (Ibid. Bd 31, 1930.)

Dickson, L. E. *History of the theory of numbers.* (Vol. II, ch. XX pp. 533—539 and vol. III, ch. XII.)

Fueter, R. [1] *Über kubische diophantische Gleichungen.* (Comm. Math. Helv. vol. 2, 1930.)

Lagrange, J. L. [1] *Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers.* (1770, Euvres t. 2.)

Landau, E. and Ostrowski, A. [1] *On the Diophantine equation* $a y^2 + b y + c = d x^n$. (Proc. London Math. Soc., vol. 19, 1920.)

Levi, F. [1] *Kubische Zahlkörper und binäre kubische Formenklassen.* (Ber. d. Sächsischen Ges. d. Wiss., Math.-Phys. Klasse, Bd 66, 1914.)

Ljunggren, W. [1] *Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante.* (Acta Math., Bd 75, 1942.)

Mordell, L. J. [1] *The Diophantine equation* $y^2 - k = x^3$. (Proc. London Math. Soc. vol. 13, 1913.) [2] *Note on the integer solutions of the equation* $E y^2 = A x^3 + B x^2 + C x + D$. (Messenger of Math., vol. 51,

1922.) [3] *On the rational solutions of the indeterminate equations of the third and fourth degrees.* (Proc. Cambridge Philos. Soc., vol. 21, 1922.) [4] *A chapter in the theory of numbers.* (Cambridge 1947.)

Nagell, T. [1] *Solution complète de quelques équations cubiques à deux indéterminées.* (Journ. de Math., 9e serie, t. 4, 1925.) [2] *Über einige kubische Gleichungen mit zwei Unbestimmten.* Math. Zeitschr., Bd 24, 1925.) [3] *Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante.* (Ibid. Bd 28, 1928.) [4] *L'analyse indéterminée de degré supérieur.* (Mémorial des Sciences Math., L'acad. des Sc. de Paris, fasc. XXXIX, 1929.) [5] *Sur les propriétés arithmétiques des cubiques planes du premier genre.* (Acta Math., Bd 52, 1929.) [6] *Zur Theorie der kubischen Irrationalitäten.* (Ibid. Bd 55, 1930.) [7] *Einige Gleichungen von der Form* $ay^2 + by + c = dx^3$. (Vid. Akad. Skrifter, Oslo, I 1930 nr 7.) [8] *Über die Lösbarkeit gewisser diophantischen Gleichungen dritten Grades.* (Comm. Math. Helv., vol. 9, 1936.)

Reid, L. W. *Tafel der Klassenzahlen für kubischen Zahlkörpern.* (Diss. Göttingen 1899. Abstract in Amer. J. Math. 23, 1901.)

Skolem, Th. [1] *Diophantische Gleichungen.* (Erg. d. Math. 5:4, 1938).

Thue, A. [1] *Bemerkungen über gewisse Näherungsbrüche algebraischer Zahlen.* (Vid.selsk. Skrifter, Kristiania, I 1908 nr 3.) [2] *Über Annäherungswerte algebraischer Zahlen.* (Journ. f. Math., Bd 135, 1909.) [3] *Über die Unlösbarkeit der Gleichung* $ax^2 + bx + c = dy^n$ *in grossen ganzen Zahlen* x *und* y. (Archiv for Math. og Naturv., Kristiania 1917.)